

修士論文

Empirical Studies on Regional and
Sectoral Interdependencies of Information
Security

情報セキュリティの地域間およびセクタ間
相互依存性に関する実証研究

指導教員 松浦幹太 准教授

東京大学大学院 情報理工学系研究科 電子情報学専攻

48-106414 Bongkot JENJARRUSSAKUL

平成 24 年 02 月 08 日提出

Abstract

Nowadays information technology system becomes very important in a modern business. Firms link their information technology system together in order to increase their efficiency. The linked systems help businesses communication, transact, and operate their works easier and faster. It also helps reducing cost and time. These are important advantages which make information technology becomes backbone of worldwide businesses.

In this paper, first we discuss the problem and background knowledge of information security management. We talk about general viewpoints on economics of information securities. Here research catagories in information security economics will be presented with some interesting examples.

Then we talk about motivation of the research in interdependency of information security. Here we try to give readers some viewpoints of interdependency of information security from both sectoral and regional viewpoints.

Next we present our way to propose the empirical study on the sectoral and regional interdependency of information security. Our empirical study shows differences of interdependency of information security in both perspectives. Moreover we also discuss about the interdependency of information security according to our results in a comprehensice manner due to our objective of this empirical study.

We also show result regarding informat impact on interdependency of information security due to the Great East Japan Earthquake. The results show some reduction in interdependency of information security due to this large scale earthquake. Such reduction in interdependency of information security might refer to sensitivity of the security.

Contents

Abstract	i
1 Introduction	1
1.1 Information Security Economics	1
1.1.1 Four types of concern in information security economics	2
1.1.2 The Motivation of Interdependency of Information Security	5
1.2 Our Contributions	6
1.3 Organization	7
2 Related Literatures	8
2.1 Interdependency from sectoral perspective	8
2.2 Interdependency from regional perspective	14
3 Methodology	17
3.1 Analysis of Structural Interdependency	17
3.1.1 Observed Values	18
3.1.2 Backward Dependency (BD) and Backward Linkages (BL)	21
3.2 Analysis of Interdependency under Influence of Information Technology and Information Security	23
4 Study on Japanese Industrial sector and region	26
4.1 Data	26
4.2 Variables for information technology and information security	31
4.3 Regional and sectoral production values	37
5 Impact from the Great Japan Earthquake	41
5.1 Study on Impact from the Great East Japan Earthquake	42
5.2 Analysis the impact on structural interdependency	43
5.3 Additional data for the study on impact from the Great East Japan Earthquake	43
5.4 Variables for impact estimation	44
5.5 Estimation of the effects from an investment in information security	45

6	Results and discussion on Interdependency of Information Security from the Empirical Study	47
6.1	Sectoral and regional interdependency of information security·····	48
6.1.1	Sectoral interdependency of information security ·····	49
6.1.2	Regional interdependency of information security ·····	53
6.1.3	Discussion ·····	54
6.2	Impact from the Great East Japan Earthquake on information security··	61
6.2.1	Result of changes on output·····	61
6.2.2	Result of changes on interdependency of information security·····	63
6.2.3	Discussion ·····	64
7	Conclusion	66
	Acknowledgements	69
	Bibliography	70
	Publications	75
A	Results for study on sectoral and regional interdependency of information security	76
B	Results for changes on interdependency of information security	86

Chapter 1 Introduction

1.1 Information Security Economics

Information security has long been employed in the information technology system. With speedy adoption rate of the information technology system in basic infrastructures as well as businesses, information security becomes very important. One main reason that make information technology system becomes one of the most important infratructures in business world is that it links businesses together by using various kinds of information technology links. We could say that information technology system becomes backbone of many modern businesses.

Information security helps users of the information technology system reduce their rate of lost due to fraud, information threat, spam, plishing, and other kinds of attacks that aim to harm their information technology system. The scale of lost from attacks can be in any scale from large to small. In fact, not only to the information system itself, the lost from attacks might occur with any information contents which might not be able to estimate in a value. For example lost of personal information or confidential contents. The businesses with such lost might also lost thier business opportunitites and reliability in the business market. These are main problems that lead to the necessity of information security economics.

Although many firms concern problems regarding information security, but due to worldwide economic recessions, they might inappropriately invest in information security[26]. Moreover the worldwide economic recessions is one of the factors which raises number of cyber crime. Hence many firms concern on information security investment. In fact there are higher number of firms and organizations that concern more about expenditure on information security.

In addition, some firms might under- or over-estimate the effects of information security attacks. Hence firms that under-estimate the effects of information security attacks might not consider or invest much in information security. So its information security system might not strong enough to handle some kind of attacks. If attackers can find any weak points in the system, they can easily attack and harm the system of under-investment firms. On the other hand, firms that over-investment in information security of its system might spend too much on the system. So that they might not effectively gain high benefit from their investment.

In my opinion, these problems are important and lead to the investors as well as governments whether they appropriately spend or invest in information security in order to secure their information system or not.

From these facts, the understanding in other aspects such as economics are also required beside the understanding in information technology system and information security. With these combinations and appropriate decisions, it would be more sufficient for appropriate adoption in information security on designate system. These are only some important reasons which bring necessity of information security economics.

1.1.1 Four types of concern in information security economics

The failure of information security can be caused by many types of threats. In 2006, Anderson and Moore categorizes researches in information security economics into 4 main categories[34]. Each category is grouped based on applications of economic theories and ideas to solve similar type of information security problems. Some interesting studies are shown to give ideas for each category.

Misaligned Incentives The concepts of economic theories are used to show that a hidden action problem arises when one of two parties, who want to transact, take unobservable actions that affect the outcome. Or we could say that there are hidden action attacks within the system.

In 1994, Anderson introduced a study on misaligned incentives by observing the retail banking systems[32]. He uses the economic concept of *Moral hazard*¹ to explain the failure which occurred in retail banking systems. He states that instead of lack of protection or having technical weakness in the system, the attacks came from the fact that the bank did not use available products properly. Hence attackers could attack at the hole which came from such basic error. He concludes that most frauds in the banking system were not caused by cryptanalysis or other technical attacks, but by human errors and failure in management.

Varian presented another simple example on this concept via his article in 2001[10]. He said that users are normally willing to pay for antivirus in order to protect their own computers but not likely to spend for the cost of the attack on someone else. Such behaviours lead to some hidden weak points in the whole information system. Hence attackers might attack the system via those hidden weak points.

¹**Moral hazard** is a principle which presents the risk at the time two parties come into agreement with one another. At that time, each party might take a chance to gain from acting differently from what it should behave so that it brings risk into the system. It can be reduced by the placing of responsibilities on both parties of a contract[15].

Network Externality Actions of individuals can cause side effect on others. This category emphasizes on relationships between individuals and/or firms. The effect from actions of each individual can be both positive and negative.

In information security, increment or decrement of investment in information security in a firm can affect its partners via their interconnections. That is because information system has become one of common infrastructures[24]. Moreover it might also lead to some problems such as problem of under- or over-investment in the information security system.

In 2001, Anderson presented a study on network externality in [33]. He pointed three important features of information technology markets to explain consequence problems. Moreover he also provided suggestion on direction which can help fixing problems. These three important features of information technology markets are:

1. Value of a product depends on number of users.
2. Technology usually has high fixed costs and low marginal cost.
3. Large costs to users from switching technologies are often required.

These features bring problems of vendor locked-in as well as switching cost into the system. Hence although users of the information notices that there are some weaknesses within the system, it might be difficult to persuade users to change their systems. One of Anderson's technical suggestion due to this problems is to make security administrative be more user-friendly or using the concept of plug-and-play.

Economics of Vulnerability In 2006, Anderson et al. explained that vulnerability market is the system which helps buyers and sellers establish the actual cost of finding a vulnerability in the software[34]. This market helps providing information regarding vulnerability of the released software or system. Hence the advantage of vulnerability market serves both customer and vendor of the affected products.

While vulnerability market aims to provide information about vulnerability to their customers, which are both user and vendor, cyber-insurance depends on insurer who sets the premium based on firm's IT infrastructure.

Böhme and Kataria introduced the topic regarding Cyber-Insurance[28] in the same year. In their work, they introduced the use of correlation of cyber-risks to classify the type of cyber-risk based on twin-tier approach. The first type of cyber-risk is the correlation of cyber-risks within a firm. For example failure of multiple systems within an internal network. Another type is the correlation of cyber-risks at a global level. For example the infection of worm like Code red worm in year 2001 that simultaneously

attacked wide range of organization. With these classifications, global risk correlation influences insurers' decision setting the premium. On the other hands, the correlation of cyber-risks within a firm (so-called internal correlation) influences its individual decision to seek insurance.

Economics of Privacy Economics methodologies within this category copes with the problems related to erosion of personal privacy within the information system. They help explaining why privacy-enhancing technologies failed in the marketplace.

In 2003, Vila et al. defined "protecting privacy" according to the fair information practices principles provided by Federal Trade Commission[39]. Their work focused on the information about vendor which are available to customers. They mentioned that the privacy in websites is similar to lemon market.² Users do not know whether their chosen websites respect users' privacy or not. "Privacy signals" was introduced in this study as a result of motivation from lemon market for privacy. Customer can use privacy signals to tell the differences between website with privacy-respecting and privacy-defecting website. The signal that the website's owner try to provide to their customers might come from a long privacy policy or the use of P3P policy.³ This study can be conclude by using instability in the privacy market known as "Instability Cycle" in figure 1.1. By using Instability cycle, they concluded that if the customer trust in seller's security, seller does not necessarily invest in information privacy.

Another interesting research under this category was introduced by Odlyzko in 2003 in [2]. He introduced research on price discrimination and privacy. Odlyzko used an economic concept of price discrimination to explain why do people care about privacy and its erosion. He pointed out that in internet environment, there will be higher incentive on price discrimination. That is because, there is high motivation for vendor on reducing customers' privacy and gain their customers' information. Those customers' information will be used by private sector to provide charge in different price to customers for the same goods or services. So that the erosion of privacy allows private sectors to learn more about their customers such as their willingness to pay, age of the customers, the size of customers (whether they are large, medium, small enterprise or an individual), etc. The study in such this topic will help understanding the problems and help increasing efficiency of the economy. Moreover personalized services in information security can be provided with low marginal cost.

²**Lemon market theorem** was introduced by Akerlof in 1970. This theorem is based on a concept of asymmetry information where seller knows more about their product than its customer.

³**P3P policy** is a protocol designed to inform web users of the data-collection practices of the websites.

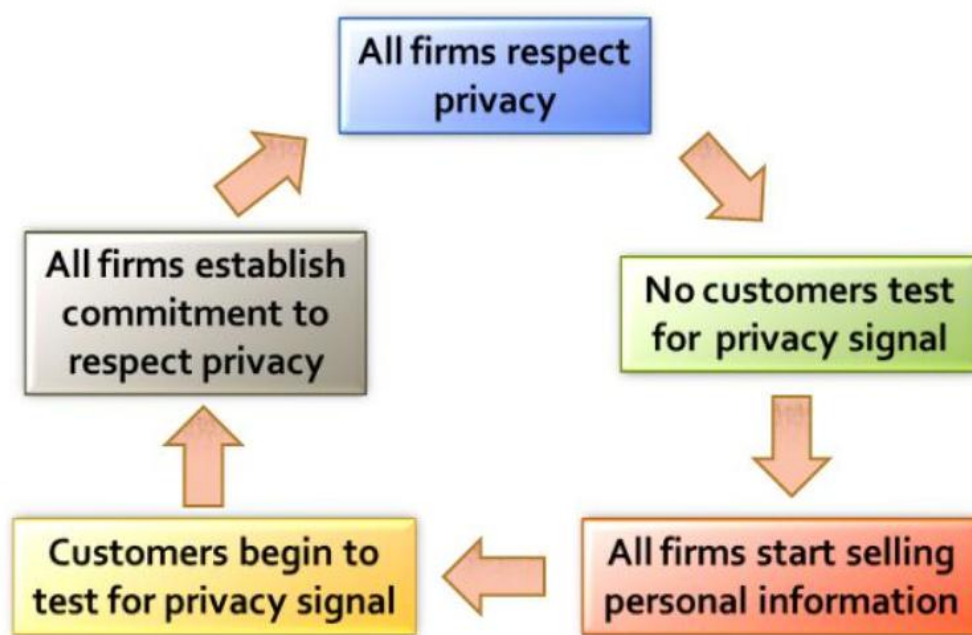


Figure 1.1: Instability Cycle

1.1.2 The Motivation of Interdependency of Information Security

Interdependency of Information Security is one of the studies in Network External-ity. An empirical study on interdependency of information security requires 2 main groups of knowledges. The first group is a knowledge in economic perspective and another group is in information security perspective. To do so, the combinations between information security and economic will help investors of an information system appropriately make their decision on designate system with appropriate budget.

Interdependency in economic perspective

For interdependency of economic activity, information technology becomes one of the role players in business-to-business (B2B) firm supply chains[31]. It bring interdependency of economic activity into many industrial sectors such as automotive[17], computer[16], financial services[3][7][21], and retail and logistics[6][35][44]. These industrial sectors operate their transaction through business-to-business infrastructure such as electronic data interchange (EDI) to exchange information among supply chain partners[29][36]. EDI system helps those organizations reach their target faster by the exchange in information[29].

Interdependency of information security

For interdependency of information security, Anderson, et al. stated that interdependency regarding information security is one of the study on economic externalities[34]. Kunreuther and Heal apply Nash equilibria to assess the interdependent security which is the type of interaction between agents on information security investment[13]. The study of impact of network security vulnerability and supply chain integration on firm's incentives to invest in information security is introduced by Tridib, et al.[38]. They show that the degree of network vulnerability or the degree of supply chain integration has relations to security investments of the firms. Hausken provides framework in which two interdependent firms will be both impacted by security investment and attacks if their interdependence increase[20]. Ogut et al. show that the interdependence of cyber-risk reduces firms' incentives to invest in security technologies as well as to buy insurance coverage[14].

The improvement in information technology becomes one of main factors that increased interconnectedness and interdependencies of critical infrastructures, such as telecommunication, banking and finance, transportation, and continuity of government. Moreover impact regarding natural phenomena like earthquake, hurricanes, or tsunami as well as matter regarding acts of terrorism also become important concerns. Understanding in complex and interconnectedness among them drastically shows an important due to these concerns[43].

1.2 Our Contributions

Our contribution is to analyze characteristics of interdependency of information security in sectoral and regional perspectives by using Japanese official data. By this we focus on interdependency of information security from demand-side perspective. In economic viewpoint, demand-side perspective is important because the demand from demand-side firms initiate the needs of production and stimulate economic growth with no inflation. That is because demand-side economic, production will be varied according to the need from demand-side firms.

Although previous studies of inter-sectoral interdependency of information security demonstrated that the differences between industrial sectors is one of the factors that affect interdependency of information security. However there is no empirical study on the differences between their locations. Hence we broaden the concept of measurement methodology of interdependency of information security so that it can be used to analyze both sectoral and regional interdependency of information security.

Another contribution is to find some reduction of interdependency of information security due to the impact from the Great East Japan Earthquake. The study from this impact helps us learn more about the change due to some damages on supply-chain. Therefore we can study more about effect on interdependency of information security if the demand is reduced by some incidents. Moreover we expect that the result of this part will help supporting our result and what we could find in the first part of this work.

We discuss our results from the empirical study by considering sectoral results and regional results. With our method, we could see some significant characteristics which is belonged to each industrial sectors and regions. We expect that characteristics of interdependency of information security which we discuss in this paper will help investor of the information technology system and information security properly find their investment strategy due to their type of business and business location.

1.3 Organization

In the following sections, we will summarize related works in chapter 2. The methodologies, which we used to test interdependency of information security, as well as data and study on Japanese industrial sectors and regions will be in chapter 3 and chapter 4, respectively. The method to study on impact from the Great East Japan Earthquake is in chapter 5. After that we will talk about the results with some discussions in chapter 6. Finally we will give the conclusion in chapter 7.

Chapter 2 Related Literatures

Our empirical study on interdependency of information security aim to find both interdependency from sectoral and regional perspectives, hence related literatures in this chapter will be grouped and introduced according to their perspective.

2.1 Interdependency from sectoral perspective

One of the methodologies for analyzing interdependency in the context of inoperability is the Inoperability Input-Output Model (IIM). Inoperability Input-Output Model is a Leontief-based infrastructure input-output model. It was introduced by Haimes and Jiang [43]. The IIM is an analytic framework to quantify and address the risks from the intra- and inter-connectedness of economic and infrastructure sectors [37]. It can be shown as in figure 2.1. Hence this model is used to ensure the integrity and continued operability of complex critical infrastructure which is in the aspect of physical-based model.

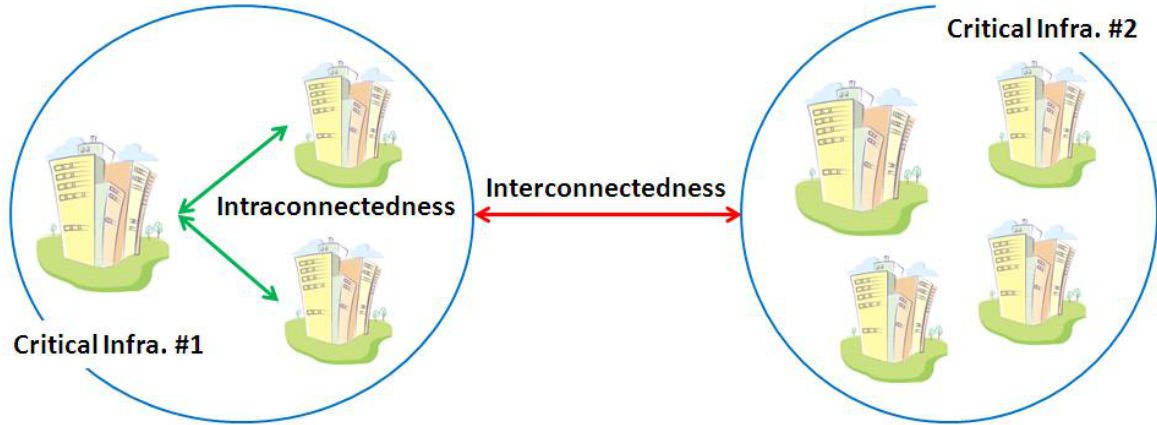


Figure 2.1: Inoperability Input-Output Model (IIM)

Subsequence of IIM studies (e.g.[18][19][40][41]) used economic-based data and model to study physical interconnectedness.

In information security, IIM model was used to examine IS interdependency in many studies such as in [9], [19], and [42].

Intedependent infrastructure sectors and IIM model In 2005, Haime et al. discussed the theory and methodology supporting the development of the IIM model in [40]. *Inoperability* in *Inoperability Input-Output Model* is defined as “the inability of the system to perform its intended natural or engineered functions”. It can be referred to the level of the system’s dysfunction, deccribed in percentage of the system’s as-planned level of operation.

The main objective of their model is to assess impact on the system due to complexity of the system or interdependencies between infrastructures. The impact is mainly applied in the scope of *physical and economic losses*. However it can also extend to cassess impacts due to information failure.

By this, they consider n critical connected industrial sectors and assess the output which is their inoperability that is caused by any harmful incident in one or multiple industrial sectors.

The use of IIM in this work focus on “*industry-by-industry*” viewpoint. Althought they also mentioned the use of *regional data*, it only refers to data which shows values indicates interdependencies from a specific region in a country. This mean IIM model is originately use to find interdependencies between industrial sectors rather than interdependencies between locations¹.

Haime et al. introduced the formular of the physical-based model by adding superscript P into the original formulation by Leontief. Rather than measure in production or manetary units for commodities as in Leontief’s original model, Haime et al. also interpret their model in a different way. Their formula can be shown as follows:

$$x_i^P = \sum_j a_{ij}^P x_j^P + c_i^P \Leftrightarrow \mathbf{x}^P = \mathbf{A}^P \mathbf{x}^P + \mathbf{c}^P \quad (2.1)$$

where

- \mathbf{c}^P represents the *input* to the interconnected infrastructues. It is a final demand for the i^{th} industry.
- \mathbf{A} represents Industry-by-Industry technical coefficient matrix. It tells the distribution of input contributed by various industries $i = 1, 2, \dots, n$ (production) to the total inputs required by industry j (purchaser).

¹In Haime et al.’s work, they consider interdependencies between industrial sectors in the United States. They found that interregional feedbacks from their empirical study seems to be small. However, input-output analysis for a particulr region shows more accurate analysis of interdependency for a specific region.

\mathbf{x}^P represents the *output* which is a *resulting vector of inoperability* of the different infrastructures due to their connections to the troubled infrastructure and to one another.

The inoperability vector \mathbf{x}^P has values between 0 and 1. $\mathbf{x}^P = 0$ is a flawless operation. The infrastructures are said to be *as-planned* in *ground-state* when it met this value.

When consider *regional IIM*, the technical coefficient matrix \mathbf{A} has to utilize *location quotients* which indicates *how well an industry's production capacity can serve the regional need*. The location quotients is defined as

$$l_i = \frac{\hat{x}_i^R / \hat{x}_s^R}{\hat{x}_i / \hat{x}_s} \quad (2.2)$$

where

\hat{x}_i^R is the regional output for the i^{th} industry.

\hat{x}_s^R is the total regional output for all regional-level industries.

\hat{x}_i is the national output for the i^{th} industry.

\hat{x}_s is the total national output for all national-level industries.

If the value of l_i tends to 1, its relative concentration in the region approaches that of the national level. The regional industry-by-industry technical coefficient matrix \mathbf{A}_R , whose elements are denoted by a_{ij}^R , is then calculated by:

$$a_{ij}^R \equiv \begin{cases} a_{ij}(l_i) & l_i < 1 \\ a_{ij} & l_i \geq 1 \end{cases} \quad (2.3)$$

In addition, Haime et al. also introduced “Dynamic IIM” which used to test interdependency with temporal dynamic behaviour of industry recoveries. To do so, *industry resilience coefficient* is introduced.

The equation for dynamic IIM can be shown as follows:

$$\dot{x}(t) = \mathbf{K}[\mathbf{A}\mathbf{x}(t) + \mathbf{c}(t) - \mathbf{x}(t)] \quad (2.4)$$

where

\mathbf{A} is the Leontief technical coefficient matrix.

$\mathbf{c}(t)$ is the final demand vector at time t .

$\mathbf{x}(t)$ represents the total output of sectors at time t .

\mathbf{K} is the industry resilience coefficient matrix whose each element of k_i represents the resilience of sector i . When there is an attack, k_i measures the recovery rate of the industry sectors.

Then they transform equation 2.4 into the normalized inoperability form as follows:

$$\dot{q}(t) = \mathbf{K}[\mathbf{A}^* \mathbf{q}(t) + \mathbf{c}^*(t) - \mathbf{q}(t)] \quad (2.5)$$

where

\mathbf{A}^* is the normalized interdependency matrix.

vector $\mathbf{c}^*(t)$ is the normalized final demand vector at time t .

$\mathbf{q}(t)$ is the inoperability vector at time t .

The vector $\mathbf{c}^*(t)$ can be adjust due to the impact of the attack. When there is an impact, demand perturbation vector is needed in order to describe normalized final demand vector under impact of the attack. To do so, we have to generate a normalized use matrix (denoted by $\hat{\mathbf{U}}$) by dividing each element of the use matrix (u_{ij}) by its respective column sum (in figure 2.2, the column sum is the value of Total Industry Input (x^r)).

For more understanding, *make* matrix shows the monetary values of the different column commodities produced by the different row industries. In contrast, *use* matrix shows the monetary values of the different row commodities consumed by the different column industries. In another word, use matrix is a commodity-by-industry matrix which captures the value of the i th (row index) commodity used by the j th (column index) industry ($u_{i,j}$), or by each final user. Conceptual economic input-output table which *make* and *use* matrix refer to can be shown as in figure 2.2.

Then we find the value of normalized final demand as follows:

$$c_j^* = p_i \frac{\hat{u}_{ij}}{\hat{u}_{i,max}} \quad (2.6)$$

where

c_j^* is perturbation to industry j due to inoperability of commodity i .

p_i is perturbation to maximum consuming industry of commodity i due to inoperability of commodity i ².

\hat{u}_{ij} is normalized use of commodity i by industry j .

$\hat{u}_{i,max}$ is normalized use of commodity i by maximum consuming industry.

They replace this new value of c_j^* into 2.5 to calculate the impact from the attack. During the recovery time, the inoperability of commodity is expected to be decreased. Hence they can find the trade-off value of commodity recoveries in a specific time-frame (e.g. 10, 30, 60 days). According to their work in [41], they use high-attitude electromagnetic pulse (HEMP) attack scenarios on some industry to prove their model.

	Commodity	Industry	
Commodity		Use Matrix (U)	Total Commodity Output (y)
Industry	Make Matrix (V)		Total Industry Output (x)
	Total Commodity Input (y^r)	Total Industry Input (x^r)	

Figure 2.2: Overview of economic input-output table adapted from [40].

The HEMP is an intense electromagnetic blast induced from high-elevation nuclear explosions which can cause damage to electronic and electrical systems.

One of their empirical cases is that they set 60-day as their time-frames and find effect from HEMP attack scenario on power industry. First they find 10 most affected industries due to the lost from the attack. Next they relationships between inoperability of power sector (%), recovery time (60-day), and total economic loss. They found that if the sector takes long time for its recovery, there will be more total economic loss. On the other hand, if the sector can be recovered in a higher speed, the inoperability will drop faster and will lead to less total economic loss.

Hierarchies of cyber security metrics and IIM model[37] Application with the IIM framework can be used to integrating analyses of systems as a view from different hierarchies that include both economic interdependency and physical interdependency as shown in figure 2.3.

The hierarchical pyramid shows how economic and physical systems interact. The top half of the pyramid represents industry/regiona/national-level economic metrics. This top half gives us a whole picture of national security. On the other hand, the bottom half show plant-level process control system security metrics. This part is the foundation of SCADA ³ security. This is why IIM can be used to analyze interdepen-

³SCADA or Supervisory Control And Data Acquisition is used in utilities industry in the U.S.

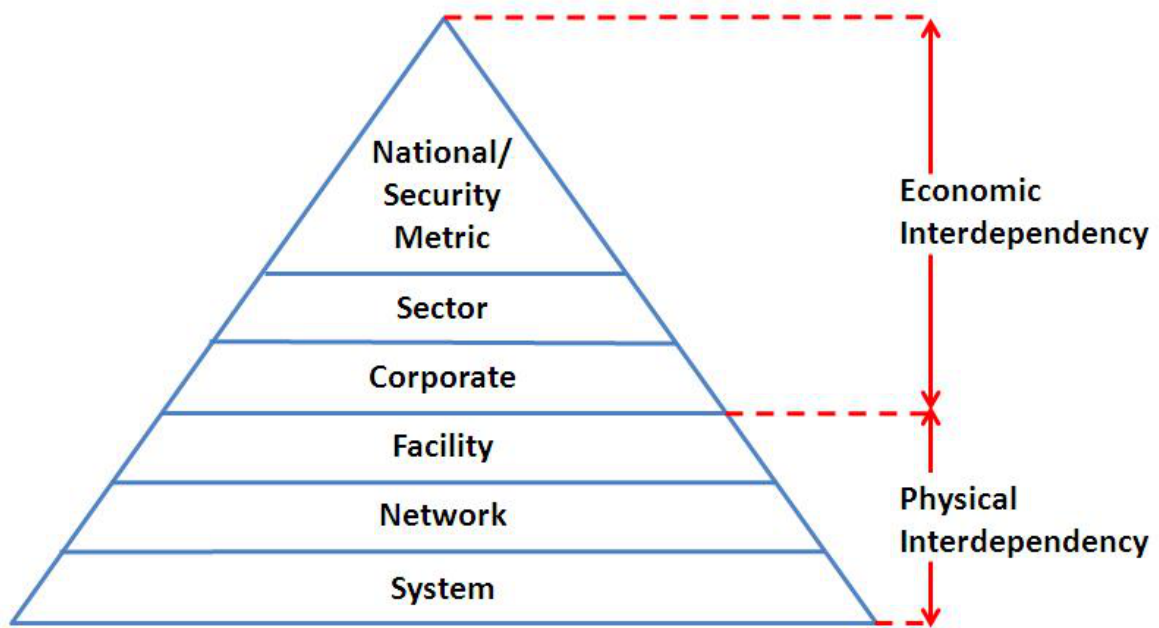


Figure 2.3: Framework for Linking Hierarchies of Cyber Security Metrics[37].

dency in the information security perspective.

In fact, the framework for linking hierarchies of cyber security metrics in [25] is used to show consequent risks when there is cyber attack in any industrial sector (in this work, they set cyber risk scenario on industrial sector of Oil and Gas Industry). Quite similar to the research in [40], this framework also mention “*ripple effects*”.

The consequent risks act as ripple effects on related critical infrastructures such as transportation, telecommunications, energy, and banking. Moreover the cyber risk which occur on the group of sectors which has physical interdependency will at last give ripple impact on economic interdependency between related industrial sectors as shown in figure 2.4.

Limitations of Inoperability Input-Output Model (IIM) However there are two main limitations. The first limitation is that IIM does not distinguish backward linkage (BL) and forward linkage (FL) which are the analysis of cross-sector linkage measures. This mean that IIM does not show differences between demand-driven perspective and supply-driven perspective[12]. Another limitation is that there is no consideration along with data regarding information technology and information secu-

to monitor critical infrastructure systems and provide early warning. In addition, SCADA also has ability to evolve with information technology (IT) systems. Moreover SCADA systems include components and subsystems which may be vulnerable to malicious cyber attacks[25].

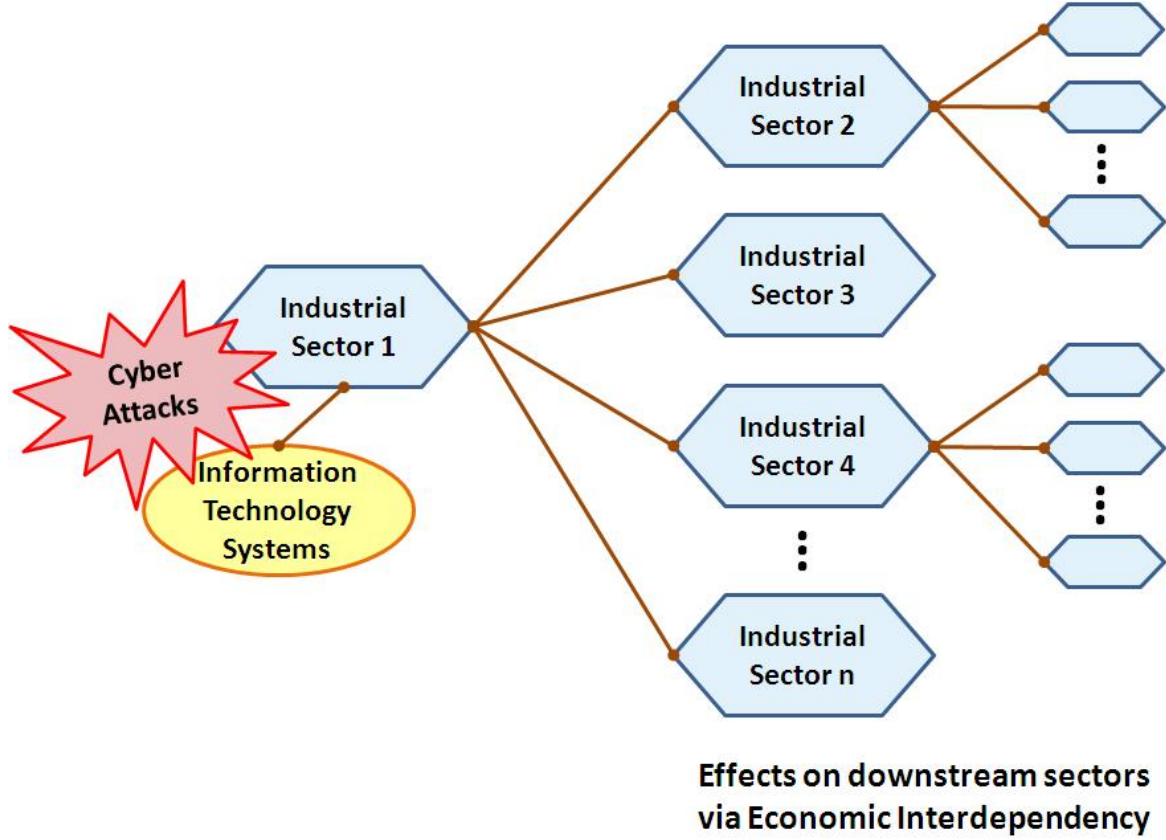


Figure 2.4: Downstream sector ripple effects adapted from [37].

rity since only economic transaction[9][19] and capital flows[42] was consider in previous studies although they mentioned cyber-attack in the studies.

2.2 Interdependency from regional perspective

Not only interaction and dependency between industrial sectors that can effect interdependency of information security, industrial location also give some effects as well. In 2007, Tanaka shows empirical results on the assessment of the influence of business location on information security effort[11]. His study shows that the some industries are affected by the location and some industries are affected by their characteristics more than a location.

There are 47 prefectures across Japan. Amongst this number information services sector is highly concentrated on metropolitan areas, especially Tokyo and Kanagawa prefecture. To study an influence from business location, Tanaka analyzes the regional Input/Output relations in information services sector. He set 4 hypotheses in order to test impacts of a location and sectoral characteristics on security effort. These

hypotheses are:

- H₁ : A location affects firm's security effort.
- H₂ : Sectoral characteristics affect firm's security effort.
- H₃ : For the security sensitive industry, a firm's location would not affect security effort.
- H₄ : For the security-less-sensitive industry, a firm's location would affect security effort.

He tests his hypotheses by using available Japanese official statistic data which are:

1. Annual IT survey conducted by Ministry of Economy, Trade and Industry (METI), the Government of Japan.
2. Annual Information Services Survey also conducted by METI.

For hypotheses H₁ and H₂, assesment on an impact of location or industry is implemented. To do this, number of regional information services sector's payrolls ($\ln ISL$) is used for a location and value of average IT expenditures' portion to total sales in each industry ($IT/Sales$) is used for an industry. These value are provided in METI IT survey. The following equation is used for the analysis.

$$M_i = \alpha + \ln IT_i + \ln ISL_i + IT/Sales_i \quad (2.7)$$

where

- M_i : firm i's number of installed security measure.
- $\ln IT_i$: natural logarithm of Information related expenditure.
- $\ln ISL_i$: natural logarithm of a number of information services sector's payrolls in the prefecture where firm i locates.
- $IT/Sales_i$: an average portion of IT expenditures to total sales in an industry that firm i belongs to.

For hypotheses H₃ and H₄, industries are divided into 2 groups which are security-sensitive industry and security-less-sensitive industry. Then location impact in each industry based can be assessed by a number of regional information services sector's payrolls as in following equation.

$$M_i = \alpha + \ln IT_i + \ln ISL_i \quad (2.8)$$

From his work, he shows 3 implications from the analysis.

1. Industry characteristics would affect firm's information security effort more than a location.
2. A location could affect firm's security effort when assessed on an industry-by-industry basis.
3. Security-sensitive industry might not be affected by a location and only security-less-sensitive industry would be affected.

For example, security-sensitive industries such as “ICT manufacturing”, “electricity, heat supply and water”, “Video picture, communications, and broadcasting”, “finance and insurance”, and “education and learning support” are industrial sectors which might not be affected by a location. In addition, these industries in a rural region seem to invest in information security at the same level as located in an urban region.

Thus, we focus on regional and sectoral interconnectedness between firms in order to realize an empirical study which follows the motivation shown in chapter 1.

Chapter 3 Methodology

Since we consider the interdependency between industrial sectors and regions in the aspect of information technology and information security, we separate our method into 2 parts.

The first part is about analysis of interdependency in economic perspective. In this part, we show how to find interdependencies between firms in across regions and industrial sectors from economic viewpoint. This part will be a basic economic methodology which lead us to the study of interdependency of information security.

The second part is about analysis of interdependency under information technology and information security influences. To make the economic methodology be able to evaluate interconnection across regions and industrial sectors, some information security related variables are needed.

By the separation of analysis methods, we will be able to see the influence of information technology and especially information security, which is our main target, over interactions between regions and industrial sectors.

3.1 Analysis of Structural Interdependency

In economic perspective, structural interdependency can be assessed in two aspects. They are demand-driven and supply-driven perspectives. In demand-driven perspective, the assessment is done from the purchaser viewpoint. On the other hand, in supply-driven perspective, the assessment is done from the producer or production viewpoint.

The assessment methodology from demand-driven and supply-driven perspectives was initially proposed by Dietzenbacher and van der Linder in 1997 in [8]. Their method is used to measure the inter-industry linkages in a multi-sectoral framework. They analyze the value of absolute *Backward Linkages* (BL) which reflects sectors' dependency on its *inputs* that they produced within the production processes. Another analyzed value is the absolute *Forward Linkages* (FL), which, in contrast, reflects sectors' dependency on its *outputs* that were sold by a particular industry to other production sectors as well as to itself.

In our work, we aim to find interdependency of information security from the demand-driven or, in another word, input-side perspective. Hence we only focus on

the concept of Backward Linkages (BL) in our analysis. In economics, demand-side economics is important because it helps stimulating economic growth without increasing an inflation. Therefore demand-side economics might also reduce the recession which is an economic problem as well.

In addition, we enhanced the basic definitions in Dietzenbacher and van der Linder's work so that they can handle both sectoral and regional perspectives.¹

3.1.1 Observed Values

Starting from input-output table. Dietzenbacher and van der Linder consider value of absolute Backward Linkages by using *input-output table* with n industrial sectors[8]. The input-output table is used to show relationships between industrial sectors in both demand-driven perspective and supply-driven perspective.

Based on their concept, we extend their definitions, added indices for regional perspective, and consider *inter-regional input-output tables* which are officially provided by Japanese government.² We select 2 sizes of datasets which are

- (1.) Inter-regional input-output table with 12 industrial sectors. And
- (2.) Inter-regional input-output table with 53 industrial sectors.

Inter-regional input-output table concludes economic data of all 9 regions with both number of industrial sectors across Japan.

As state above, data in inter-regional input-output table can be described in both demand-driven and supply-driven perspectives. In demand-driven perspective, each intersection between specific pair of industrial sector in a region refers to

$$\begin{aligned} &\text{Purchase value by} \\ &\text{companies of sector } j \text{ in region } r \text{ (column index)} \\ &\text{from} \\ &\text{companies of sector } i \text{ in region } q \text{ (row index)} \end{aligned} \tag{3.1}$$

$$\begin{aligned} d &\equiv (\text{number of regions}) \\ n &\equiv (\text{number of sectors}) \end{aligned} \tag{3.2}$$

Hence, from concept in 3.1, the observed values which we can directly observe from inter-region input-output table are presented in figure 3.1

The matrix structure for this inter-regional input-output table is denoted by

¹In Dietzenbacher and van der Linder's work, they only tested the linkages to find interdependency between demand-side and supply-side industrial sectors.

²Ministry of Economic, Trade, and Industrial (METI) under the Japanese government officially provides 3 sizes of datasets on its website. They are datasets with 12, 29, and 53 industrial sectors.

<div> <div>Purchase (Input)</div> <div>Production (Output)</div> </div>	...		Region r				...	Import (Neg) r=q i=j	Export (All regions by row)
	Sector j	...	Final Demand	...			
...	...								
...	...								
Region q	Sector i								
			$Z_{q,i,r,j}$		$f_{q,i,r}$			$-m_{q,i}$	$e_{q,i}$
...	...								
...	...								
...	...								
Value added			$C_{r,j}$						

Figure 3.1: Observed Values

$$\mathbb{K} = \begin{pmatrix} k_{1,1,1,1} & k_{1,1,1,2} & \cdots & k_{1,1,d,n} \\ k_{1,2,1,1} & k_{1,2,1,2} & \cdots & k_{1,2,d,n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{1,n,1,1} & k_{1,n,1,2} & \cdots & k_{1,n,d,n} \\ k_{2,1,1,1} & k_{2,1,1,2} & \cdots & k_{2,1,d,n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{d,n,1,1} & k_{d,n,1,2} & \cdots & k_{d,n,d,n} \end{pmatrix} \quad (3.3)$$

Where the first two indexes indicate region and sector of production group and last two indexes indicate region and sector of purchase group, respectively.

The structure of vector, which we use in this empirical study, is denoted by

$$\mathbb{k} = \begin{pmatrix} k_{1,1} \\ k_{1,2} \\ \vdots \\ k_{1,n} \\ k_{2,1} \\ \vdots \\ k_{d,n} \end{pmatrix} \quad (3.4)$$

In case of column vector, indexes indicate region and sector of purchase group while indexes in row vector indicate region and sector of production group.

With these definitions, next we directly observe following values from the inter-regional input-output table:

Inter-regional input-output table: Inter-regional input-output table are denoted by matrix \mathbf{Z} .

$$(\text{each element of } \mathbf{Z}) \equiv z_{q,i,r,j} \quad (3.5)$$

Each element of the inter-regional input-output table is *intermediate value*. Intermediate delivery is value of economic transaction between specific pair of production side and purchase side in the inter-regional input-output table. This is the first observed value which we can directly observe from inter-regional input-output table.

Final demand: Final demand is denoted by matrix \mathbf{F} .

$$(\text{each element of } \mathbf{F}) \equiv f_{q,i,r} \quad (3.6)$$

There are 2 types of final demand we use.

1. **Regional final demand: vector** \mathbb{F}^*

$$f_{q,i}^* \equiv f_{q,i,q} \quad (3.7)$$

2. **Accumulated final demand: vector** $\hat{\mathbb{F}}$

$$\hat{f}_{q,i} \equiv \sum_r^d f_{q,i,r} \quad (3.8)$$

In general, *final demand* is the portion of a production industrial sector's (or industrial sector i 's) total output for final consumption by end-users.

Import: Import is denoted by vector \mathbb{M} .

This is value of import in each region.

$$(\text{each element of } \mathbb{M}) = m_{q,i} \quad (: \text{ This is an absolute value}) \quad (3.9)$$

Export: Export is denoted by vector \mathbb{E} .

This is value of export in each region.

$$(\text{each element of } \mathbb{E}) = e_{q,i} \quad (3.10)$$

Value added: Value added or tax is denoted by vector \mathbb{c} .

This value belongs to each purchase group.

$$(\text{each element of } \mathbb{c}) = c_{r,j} \quad (3.11)$$

These observed values from the inter-regional input-output table with d regions and n sectors are used as fundamental values in our analysis. Next we use these values to find the backward linkages or interdependency between industrial sectors across regions from demand-driven perspective.

Let vector \mathbb{g} denotes the gross output of each input-side sector j in region r . The gross output can be obtained by

$$g_{r,j} \equiv \sum_q^d \sum_i^n z_{q,i,r,j} + c_{r,j} \quad (3.12)$$

which means all inputs from production-side and value added term become the gross output of each demand-side or input-side sector j in region r .

The normalized value of intermediate deliveries from production-side sector i in region q to purchase-side sector j in region r by gross output of sector j in region r becomes value of input coefficients. The *input coefficient* is denoted by matrix \mathbf{A} . It is defined by

$$a_{q,i,r,j} \equiv z_{q,i,r,j} / g_{r,j} \quad (3.13)$$

And the regional input coefficient is denoted by diagonal matrix \mathbf{A}^* .

$$a_{q,i,r,j}^* \equiv \begin{cases} a_{q,i,r,j} & \text{if } q = r \\ 0 & \text{otherwise} \end{cases} \quad (3.14)$$

Hence all input coefficients which belong to intermediate deliveries from production-side sectors to purchase-side sectors inside each region are shown in matrix \mathbf{A}^* .

The import coefficient is another value which is necessary in the methodology. It is an absolute value of import of sector i in region q (production-side) normalized by value of final demand of sector i in region q . Import coefficient is denoted by diagonal matrix \mathbf{B} .

$$b_{q,i,r,j} \equiv \begin{cases} m_{q,i} / f_{q,i,q}^* & \text{if } r = q \text{ and } j = i \\ 0 & \text{if } r \neq q \text{ or } j \neq i \end{cases} \quad (3.15)$$

3.1.2 Backward Dependency (BD) and Backward Linkages (BL)

To calculate value of absolute backward linkages, we assume that sector j in region r does not depend on any production sectors in any region (any sector i in region q).

This means that when the production process held constantly. all of sector j in region r 's intermediate requirements are imported from outside the region.

The reduction in output will be obtained as sector j in region r does not depend on the production sectors in any region regarding its input requirements. The reduction in output is denoted by $\mathbb{h} - \bar{\mathbb{h}}$. In another word, to find backward linkages of each sector j in region r , all devileries belong to that sector j in region r are hypothetically extracted.

The first term of \mathbb{h} refers to overall output which include the value of output when sector j in region r depends on production-side group. It is defined by

$$\mathbb{h} \equiv \{\mathbf{I} - [\mathbf{A} - \mathbf{BA}^*]\}^{-1}(\hat{\mathbf{f}} - \mathbf{B}\mathbf{f}^* + \mathbf{e}) \quad (3.16)$$

Each element is represented by $h_{q,i}$.

The second term of $\bar{\mathbb{h}}$ refers to the value when sector j in region r buys no intermediate inputs from any production group. We could say that the second term is the value when sector j in region r no longer depend on production-side group. In order to calculate this second term, we assume that the technilca production process is held constant, hence all of sector j in region r 's intermediates are imported It is defined by

$$\bar{\mathbb{h}}_{(\bar{r}, \bar{j})} \equiv \{\mathbf{I} - [\bar{\mathbf{A}}(\bar{r}, \bar{j}) - \mathbf{BA}^*(\bar{r}, \bar{j})]\}^{-1}(\hat{\mathbf{f}} - \mathbf{B}\mathbf{f}^* + \mathbf{e}) \quad (3.17)$$

where $\bar{\mathbf{A}}(\bar{r}, \bar{j})$ and $\bar{\mathbf{A}}^*(\bar{r}, \bar{j})$ are calculated from $\bar{z}_{q,i,r,j}(\bar{r}, \bar{j})$. It is defined by

$$\bar{z}_{q,i,r,j}(\bar{r}, \bar{j}) \equiv \begin{cases} 0 & \text{if } r = \bar{r} \text{ and } j = \bar{j} \\ z_{q,i,r,j} & \text{otherwise} \end{cases} \quad (3.18)$$

and

$$\bar{a}_{q,i,r,j} \equiv \bar{z}_{q,i,r,j} / g_{r,j} \quad (3.19)$$

Therefore from equation 3.16 to equation 3.19, we can see that we use the same value of gross output import coefficient when calculate value of input coefficients for both terms.

The reduction in output is in the term of the absolute backward dependence of sector j in region r on sector i in sector q . This is the dependency of sector j in region r on itself, $i = j$ and $q = r$, as well as the dependency of sector j in region r on others in following 3 cases:

- a.) $i \neq j$ and $q \neq r$
- b.) $i \neq j$ and $q = r$
- c.) $i = j$ and $q \neq r$

Let matrix \mathbf{U} denotes backward dependency (BD) of sector j in region r on production-side group. It can be calculated by

$$u_{q,i,\bar{r},\bar{j}} \equiv 100 \frac{h_{q,i} - \bar{h}_{q,i}(\bar{r}, \bar{j})}{g_{\bar{r},\bar{j}}} \quad (3.20)$$

The results come out in terms of percentage.

Let column vector $\tilde{\mathbf{U}}$ denotes the absolute backward linkage of sector j in region r . It can be calculated by

$$\tilde{u}_{q,i,\bar{r},\bar{j}} \equiv 100 \sum_q^d \sum_i^n \frac{h_{q,i} - \bar{h}_{q,i}(\bar{r}, \bar{j})}{g_{\bar{r},\bar{j}}} \quad (3.21)$$

Recall that the calculation of values in this part still have no influence or any relation to information technology and information security.

3.2 Analysis of Interdependency under Influence of Information Technology and Information Security

In this section, we show how to estimate sectoral and regional interdependencies under influences of information technology and information security on absolute backward dependency. Tanaka introduces the assumption that economic interdependency between sectors is also depended upon the information technology (IT) systems of the sectors[12].

Tanaka assumes that a malfunctioning IT system in one firm will not only affect the activities of that firm, but also those of its business partners through its effects on transactions and the provision of goods and services. By this, the terms ITBL (information technology backward linkage) which is used to reflect the level of IT dependency and ISBL (information security backward linkage) which is used to reflect the IS measures employed by each sector are introduced.

1. Information Technology Backward Dependency (ITBD) and Information Technology Backward Linkages (ITBL) ITBD (information technology backward dependency) is denoted by column vector \mathbf{V} .

$$v_{q,i,\bar{r},\bar{j}} \equiv 100 \frac{h_{q,i} - \bar{h}_{q,i}^{(v)}(\bar{r}, \bar{j})}{g_{\bar{r},\bar{j}}} \quad (3.22)$$

and $\bar{h}_{q,i}^{(v)}(\bar{r}, \bar{j})$ is defined by an equation like (3.17), where $\bar{\mathbf{A}}^{(v)}$ and $\bar{\mathbf{A}}^{*(v)}$ are calculated from

$$\bar{z}_{q,i,r,j}^{(v)}(\bar{r}, \bar{j}) \equiv \begin{cases} (1 - t_i t_j) z_{q,i,r,j} & \text{if } r = \bar{r} \text{ and } j = \bar{j} \\ z_{q,i,r,j} & \text{otherwise} \end{cases} \quad (3.23)$$

and

$$\bar{a}_{q,i,r,j}^{(v)} \equiv \bar{z}_{q,i,r,j}^{(v)} / g_{r,j} \quad (3.24)$$

where t_i = Level of IT dependency for sector i , and t_j = Level of IT dependency for sector j which are calculated from another dataset with data regarding information technology. Hence all values of interdependency between sector j in region r on production-side group in vector \mathbf{V} are values of backward dependency under influence of information technology.

Under the same concept with absolute backward linkages, ITBL (information technology backward linkages) is defined by $\tilde{\mathbf{V}}$

$$\tilde{v}_{q,i,\bar{r},\bar{j}} \equiv 100 \sum_q^d \sum_i^n \frac{h_{q,i} - \bar{h}_{q,i}^{(v)}(\bar{r}, \bar{j})}{g_{\bar{r},\bar{j}}} \quad (3.25)$$

2. Information Security Backward Dependency (ISBD) and Information Security Backward Linkages (ISBL) Similarly, ISBD (information security backward dependency) is defined by column vector \mathbf{W} .

$$w_{q,i,\bar{r},\bar{j}} \equiv 100 \frac{h_{q,i} - \bar{h}_{q,i}^{(w)}(\bar{r}, \bar{j})}{g_{\bar{r},\bar{j}}} \quad (3.26)$$

and $\bar{h}_{q,i}^{(w)}(\bar{r}, \bar{j})$ is defined by an equation like (3.17), where $\bar{\mathbf{A}}^{(w)}$ and $\bar{\mathbf{A}}^{*(w)}$ are calculated from

$$\bar{z}_{q,i,r,j}^{(w)}(\bar{r}, \bar{j}) \equiv \begin{cases} (1 - s_i s_j) z_{q,i,r,j} & \text{if } r = \bar{r} \text{ and } j = \bar{j} \\ z_{q,i,r,j} & \text{otherwise} \end{cases} \quad (3.27)$$

and

$$\bar{a}_{q,i,r,j}^{(w)} \equiv \bar{z}_{q,i,r,j}^{(w)} / g_{r,j} \quad (3.28)$$

where s_i = security risk level for sector i , and s_j = security risk level for sector j . The value of security risk level is calculated from dataset with data regarding

information security. Hence all values of interdependency between sector j in region r on production-side group in vector \mathbf{W} are values of backward dependency under influence of information security.

ISBL (information security backward linkages) is defined by $\tilde{\mathbf{W}}$

$$\tilde{w}_{q,i,\bar{r},\bar{j}} \equiv 100 \sum_q^d \sum_i^n \frac{h_{q,i} - \bar{h}_{q,i}^{(w)}(\bar{r}, \bar{j})}{g_{\bar{r},\bar{j}}} \quad (3.29)$$

However we emphasize on interdependency of information security in our study to analyze how information security in each industrial sector or each region show its characteristics regarding interdependency between each other. So the value of information security backward dependency (ISBD) is mainly focused and used in our analysis.

Chapter 4 Study on Japanese Industrial sector and region

4.1 Data

In our study on interdependency of information security, there are 3 statistical datasets which are important.

1. Inter-Regional Input-Output table for 2005 : 平成 17 年地域間産業連関表 [23]

This dataset is provided by Ministry of Economic, Trade and Industry (METI), the Government of Japan. METI officially announced 3 sizes of datasets different by number of industrial sectors (12, 29, and 53 industrial sectors) in 2005.

Generally input-output table consists of statistical data which indicate the connection between industries[27]. This table shows the transactions of all goods and services produced or sold in one year in specific regions. In Japan, the table is updated every 5 years. This table can be used to present structure of the economy, an added value and the demand structure, as well as calculating factors such as the repercussion of an economic forecast or a certain economic policy on the economy. Hence inter-regional input-output table provides statistical data between industrial sectors across 9 regions in Japan.

Here we use dataset of 12 and 53 industrial sectors to analyze the interdependency of information security. The list of industrial sectors is shown in table 4.1. Moreover we also show how dataset with 12 industrial sectors links with dataset with 53 industrial sectors. From the table table 4.1, you will find that there is no overlap industrial sectors when mapping dataset with 53 industrial sectors to dataset with 12 industrial sectors. Hence the analysis base on 53 industrial sectors will surely give us more information regarding interdepedenendy of information security in sectoral perspective.

12 Industrial sectors		53 Industrial sectors	
Sector ID	Sector name	Sector ID	Sector name
01	Agriculture	0010	Agriculture
02	Mining	0020	Mining
		0030	Coal, oil, and natural gas
03	Food and Beverage	0040	Food and beverage
04	Metal	0170	Iron and steel
		0180	Nonferrous metal
		0190	Metal products
05	Machinery	0200	General machinery
		0210	Office and service equipment
		0220	Industrial electrical equipment
		0230	Other electrical machinery
		0240	Household electric appliances
		0250	Telecommunications equipment and related equipment
		0260	Computer and accessories
		0270	Electronic components
		0280	Car
		0290	Other cars
		0300	Auto parts accessories
		0310	Other transportation equipment
		0320	Precision machinery
06	Other Manufacturing	0050	Textile industry products
		0060	Apparel and other textile products
		0070	Lumbering, wood, and furniture
		0080	Pulp, paper, paperboard, and processed paper

Table 4.1: List of Industrial Sectors.

12 Industrial sectors		53 Industrial sectors	
Sector ID	Sector name	Sector ID	Sector name
06	Other Manufacturing (Con't)	0090	Printing, platemaking, and bookbinding
		0100	Science products
		0110	Plastics
		0120	Final chemical products
		0130	Pharmaceutical products
		0140	Petroleum and coal products
		0150	Plastic products
		0330	Other manufactured products
		0160	Clay products
		0340	Renewable resources and processing treatment
07	Construction	0350	Construction
08	Utilities	0360	Electricity
		0370	Gas and heat supply
		0380	Waste water treatment
09	Commerce and Logistic	0390	Commerce
		0430	Transportation
10	Financial, Insurance, and Real Estate	0400	Finance and Insurance
		0410	Real estate
		0420	Rental housing
11	ICT	0440	Other information and communications
		0450	Information service
12	Services	0460	Public service
		0470	Educational research
		0480	Health care and social security
		0490	Advertisement

Table 4.1: List of Industrial Sectors (Con't)

12 Industrial sectors		53 Industrial sectors	
Sector ID	Sector name	Sector ID	Sector name
12	Services (Con't)	0500	Goods rental and leasing services
		0510	Other business services
		0520	Personal service
		0530	Other

Table 4.1: List of Industrial Sectors (Con't)

2. 2006 Survey of Information Technology : 平成 18 年調査関係資料 [22]

This data is also provided by Ministry of Economic, Trade and Industry (METI). 2006 survey of information technology contains sample size of 3,647 firms from 27 industrial sectors in a fiscal year 2005.

In this survey, the average number of information security measures implemented by firms in each industrial sector are collected. The average number of information security measures belongs to firms in each industrial sector as a proxy for the level of information security in each industrial sector.

Information security measures which are survey in this dataset are grouped into 4 main categories. They are listed in table 4.2.

3. Japan Industrial Productivity Database 2008 : 日本産業生産性 (JIP) データベース (JIP Database 2008)[30]

This is the last dataset which we use to analyze interdependency of information security. This dataset is provided by Research Institute of Economy, Trade and Industry (REITI).

Japan industrial productivity database 2008 contains annual data on 108 industrial sectors during 1970-2005. With this number of industrial sectors, it covers the whole Japanese economy and includes following data:

- (a) Input-output table
- (b) Capital input
 - i. Investment by sector
 - ii. IT investment by sector
 - iii. Investment matrix and stock matrix
- (c) Labor input

Hence we use data of *IT Capital Stock* and *non-IT Capital Stock* for 107 industrial sectors collected in year 2005 in our work. Data from this dataset is used to estimate *the level of IT dependency* of each industrial sector. This level can show us how does each industrial sector rely on information technology system.

Main measures category	Information security measures
Implementation of organizational measures	<ul style="list-style-type: none"> – Risk analysis – Security policy – Examination of specific measures based on security policy – Creation of information security report – Creation of Business Continuity Plan (BCP) – Deployment of an corporate-wide security management – Sectoral deployment of security management – Information security training for employees – Confirmation on information security measures of trading partners (including outsourcing)
Implementation of technical solutions/Defense measures	<ul style="list-style-type: none"> – Access control of important computer rooms – Access control of important systems – Data encryption (including Public Key Infrastructure (PKI)) – Firewall installation against external connection – Installation of ISO/IEC15408 certified product
System monitoring	<ul style="list-style-type: none"> – Installation of security monitoring software – Full-time monitoring by external professionals

Table 4.2: List of information security measures

Main measures category	Information security measures
Assessment	<ul style="list-style-type: none"> – Use of information security benchmark – Regular system auditing by external professionals – Regular system auditing by internal experts – Regular information security auditing by external professionals – Regular information security auditing by internal experts – Obtaining certification of information security management system (ISO/IEC27001)

Table 4.2: List of information security measures (Con't)

4.2 Variables for information technology and information security

For the study of information technology backward dependency (ITBD), Tanaka introduces the expression of

$$t_i = IT_i / (IT_i + nIT_i) \quad (4.1)$$

where IT_i denotes IT capital stock of sector i
 nIT_i denotes non IT capital stock of sector i in order to estimate the level of IT dependency from data in JIP database 2008[12].

Then substitute value of level of IT dependency into equation 3.23 to obtain value of backward dependency under influence of information technology.

For the case of estimation for information security backward dependency (ISBD), the level of IS measures provided in 2006 Survey of Information Technology is used. By this, Tanaka introduces the term of IS multiplier (m_i) to normalized a level of IS measures[12]. This variable is defined by

$$m_i = M^* / M_i \quad (4.2)$$

where M^* is an average number of IS measures in all industrial sectors.
 M_i is an average number of IS measures in sector i .

Another necessary variable in this study is the variable of security risk level for sector i denoted by s_i . This variable is defined by

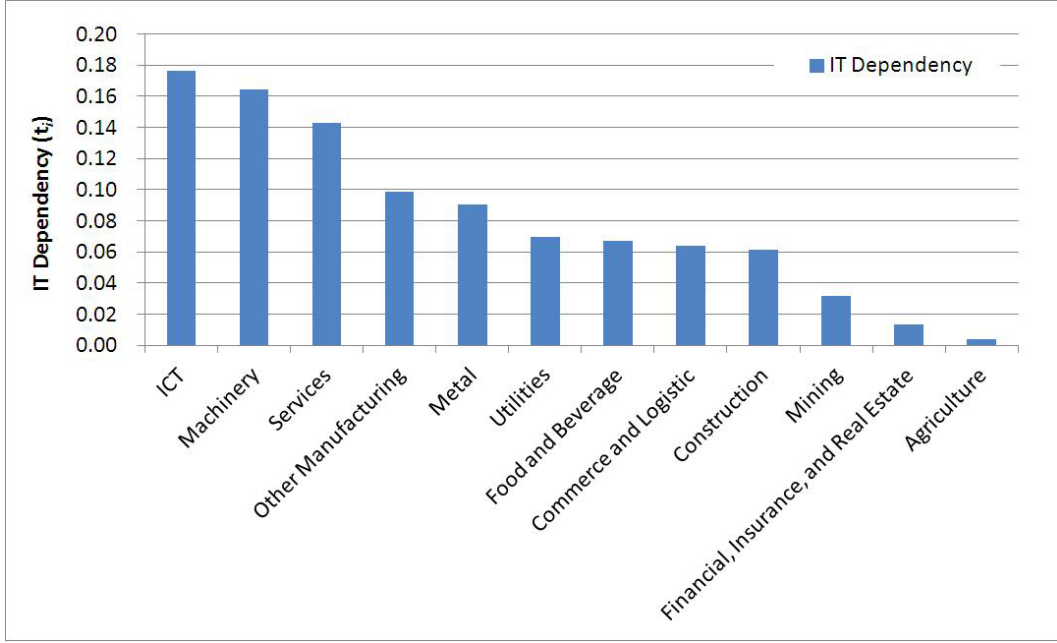


Figure 4.1: Level of IT dependency for 12 industrial sectors.

$$s_i = t_i m_i \quad (4.3)$$

where t_i and m_i are proxies for vulnerability and security investment, respectively.

Tanaka explains that t_i , which is the level of IT system vulnerability, is assumed for the possibility that it could be positively correlated to the level of IT dependency since highly IT dependent sectors are likely to be exposed to relatively more risk[12]. Then substitute variable of security risk level, s_i , into equation 3.27 to obtain value of backward dependency under influence of IS.

In our study, we apply the same level of IT system vulnerability and level of IS measures into all regions across Japan to study the influence of IT and IS dependency among industrial sectors and their regions.

Figure 4.1, figure 4.2 and figure 4.3 show level of level of IT dependency, the level of IS measures and IS multipliers and security risk level for 12 industrial sectors, respectively.

Figure 4.4, figure 4.5 and figure 4.6 show level of level of IT dependency, the level of IS measures and security risk level for 53 industrial sectors, respectively.

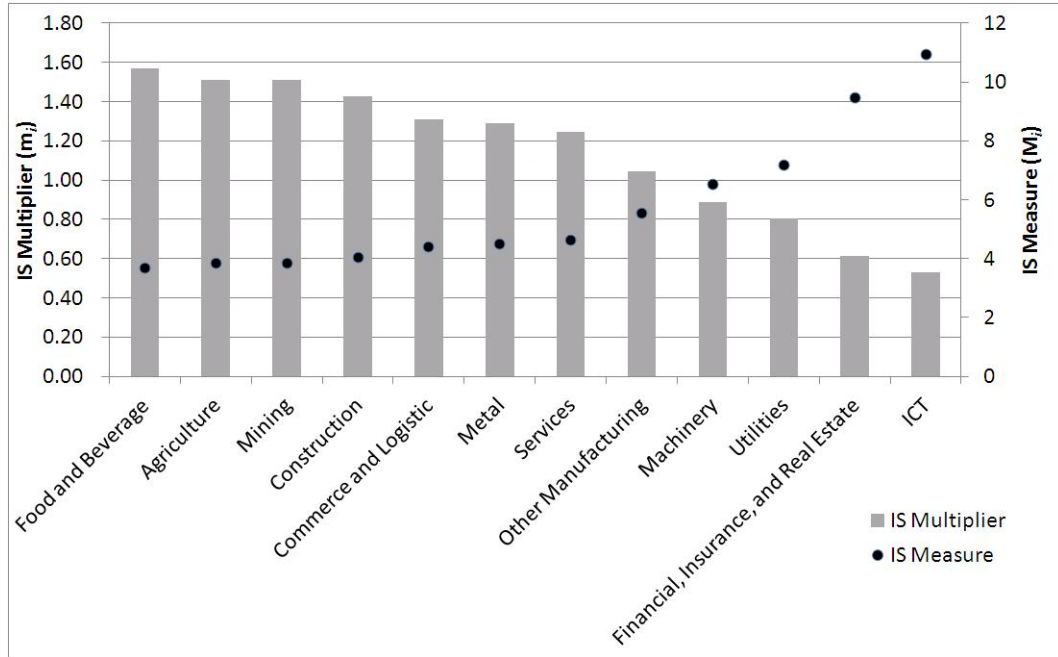


Figure 4.2: Level of IS measures and IS multipliers for 12 industrial sectors.

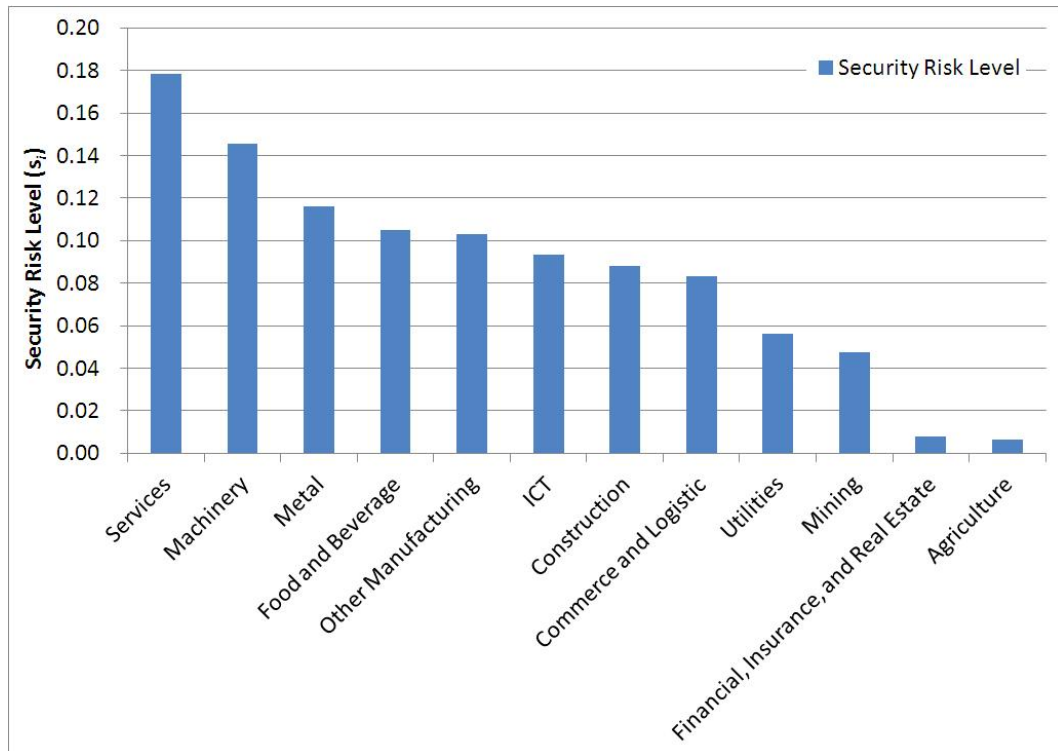


Figure 4.3: Security risk level for 12 industrial sectors.

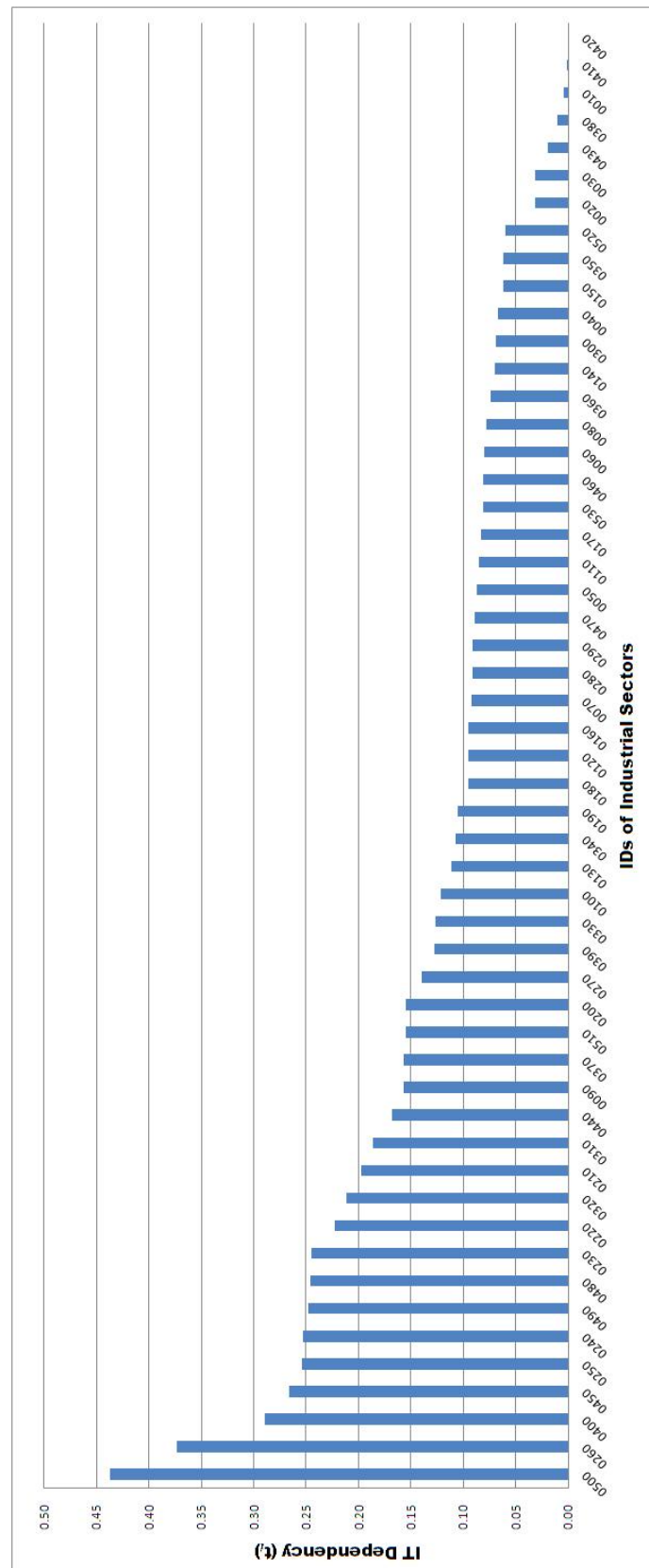


Figure 4.4: Level of IT dependency for 53 industrial sectors.

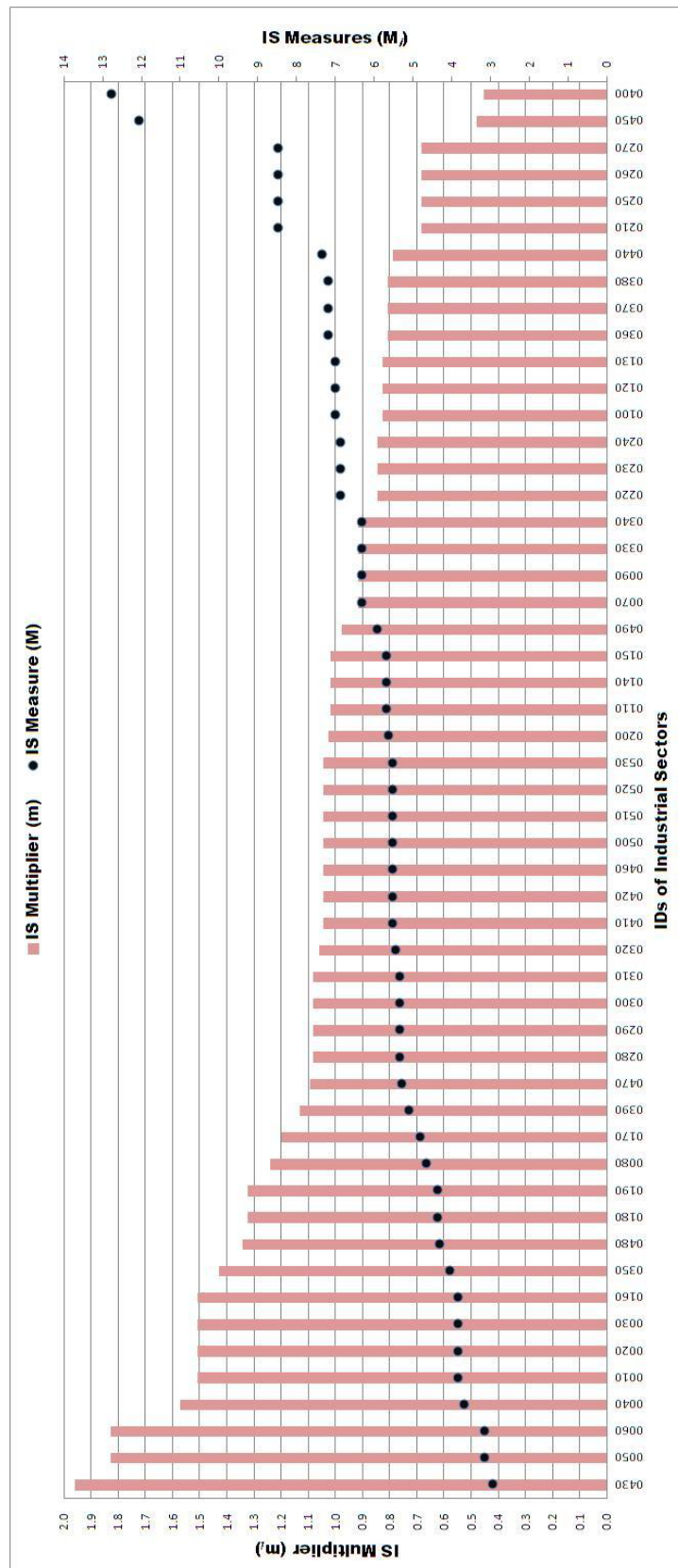


Figure 4.5: Level of IS measures and IS multipliers for 53 industrial sectors.

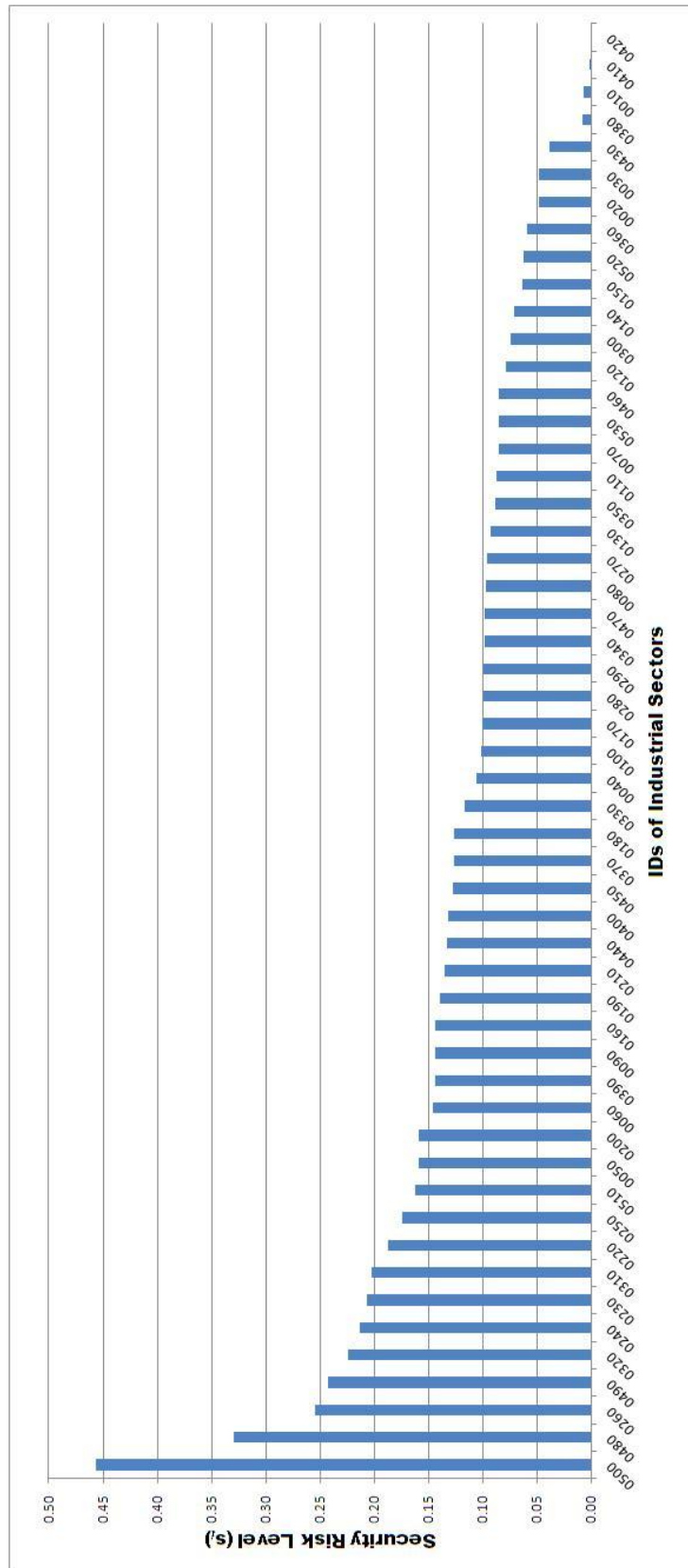


Figure 4.6: Security risk level for 53 industrial sectors.

4.3 Regional and sectoral production values

Regional and sectoral production values are one of important values. That is because, production values show the size of economic scale of each region or industrial sector. Large economic scale can refer to high economic activity inside region or industrial sector.

First, from the regional point of view, Japan is divided into 9 regions in total to collect statistical data. These 9 regions are Hokkaido, Tohoku, Kanto, Chubu, Kinki, Chugoku, Shikoku, Kyushu, and Okinawa. These regions are represented by A to I, respectively.

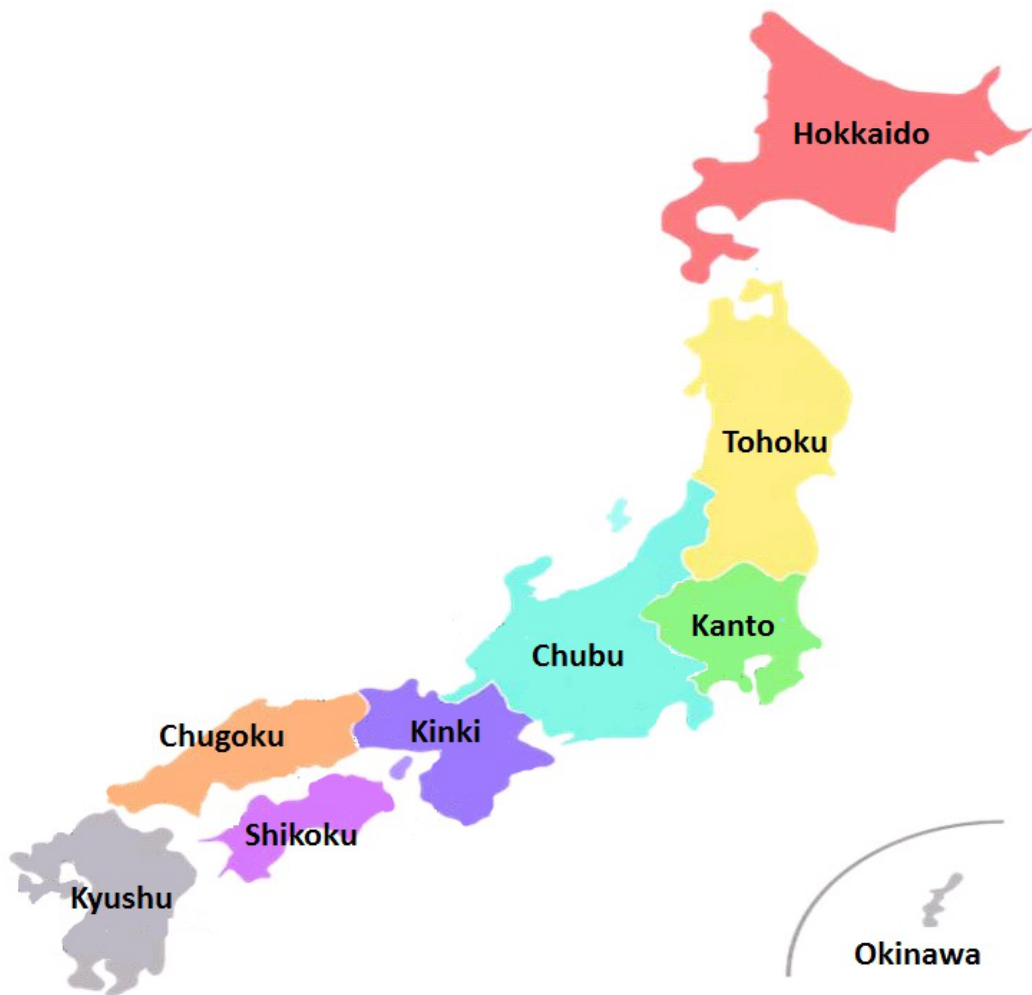


Figure 4.7: Map of Japan. Nine regions across Japan.

Table 4.3 shows the amount of production value in the aspect of region, ranked from top amount production value.

Region name	Region ID	Output (billion US\$*)
Kanto	C	8,175.19
Kinki	E	3,042.11
Chubu	D	2,341.25
Kyushu	H	1,576.64
Chugoku	F	1,176.51
Tohoku	B	1,136.39
Hokkaido	A	684.96
Shikoku	G	508.69
Okinawa	I	116.78

Source: Inter-Regional Input-Output table for 2005

*1 US(\$) = 76.75 JYP(¥). Rate on Oct 19, 11

Table 4.3: Japanese Regional Production Value.

Table 4.4 and 4.5 shows the amount of production value in the aspect of sector, ranked from top amount production value for 12 and 53 industrial sectors, respectively.

Sector name	Sector ID	Output (billion US\$*)
Services	12	3090.26
Commerce and Logistic	09	1916.02
Machinery	05	1696.06
Financial, Insurance, and Real Estate	10	1404.47
Other Manufacturing	06	1229.48
Construction	07	823.94
ICT	11	598.51
Metal	04	593.76
Food and Beverage	03	468.23
Utilities	08	349.05
Agriculture	01	171.40
Mining	02	13.14

Source: Inter-Regional Input-Output table for 2005

*1 US(\$) = 76.75 JYP(¥). Rate on Oct 19, 11

Table 4.4: Japanese sectoral production value for 12 industrial sectors.

Sector name	Sector ID	Output (billion US\$*)
Commerce	0390	1384.68
Construction	0350	823.94
Health care and social security	0480	718.11
Personal service	0520	677.81
Rental housing (imputed rents)	0420	595.16
Other business services	0510	554.62
Finance and Insurance	0400	541.85
Transportation	0430	531.33
Food and beverage	0040	468.23
Educational research	0470	440.71
Auto parts accessories	0300	373.27
Other information and communications	0440	371.76
Public service	0460	351.55
General machinery	0200	343.71
Iron and steel	0170	335.59
Real estate	0410	267.45
Information service	0450	226.75
Petroleum and coal products	0140	220.46
Electronic components	0270	211.23
Electricity	0360	205.65
Car	0280	190.51
Agriculture	0010	171.40
Metal products	0190	162.66
Goods rental and leasing services	0500	157.64
Science products	0100	138.68
Plastic products	0150	138.57
Advertisement	0490	118.35
Waste water treatment	0380	105.70
Pulp, paper, paperboard, and processed paper	0080	102.98

Source: Inter-Regional Input-Output table for 2005

*1 US(\$) = 76.75 JYP(¥). Rate on Oct 19, 11

Table 4.5: Japanese sectoral production value for 53 industrial sectors.

Sector name	Sector ID	Output (billion US\$*)
Other manufactured products	0330	101.54
Telecommunications equipment and related equipment	0250	95.51
Nonferrous metal	0180	95.50
Final chemical products	0120	94.80
Clay products	0160	93.24
Industrial electrical equipment	0220	89.33
Pharmaceutical products	0130	86.60
Other electrical machinery	0230	82.42
Printing, platemaking, and bookbinding	0090	82.03
Other transportation equipment	0310	73.62
Other	0530	71.48
Lumbering, wood, and furniture	0070	64.18
Other cars	0290	53.37
Office and service equipment	0210	52.10
Precision machinery	0320	48.50
Computer and accessories	0260	47.97
Plastics	0110	38.05
Gas and heat supply	0370	37.70
Household electric appliances	0240	34.54
Apparel and other textile products	0060	29.57
Textile industry products	0050	27.43
Mining	0020	11.54
Renewable resources and processing treatment	0340	11.34
Coal, oil, and natural gas	0030	1.60

Source: Inter-Regional Input-Output table for 2005

*1 US(\$)= 76.75 JYP(¥). Rate on Oct 19, 11

Table 4.5: Japanese sectoral production value for 53 industrial sectors (Con't)

Chapter 5 Impact from the Great Japan Earthquake

14:46 pm., March 11, 2011 - The Great East Japan Earthquake hit Tohoku region with magnitude 9.0. This massive earthquake also triggered tremendous and powerful Tsunami waves which left dreadful damages in the areas.

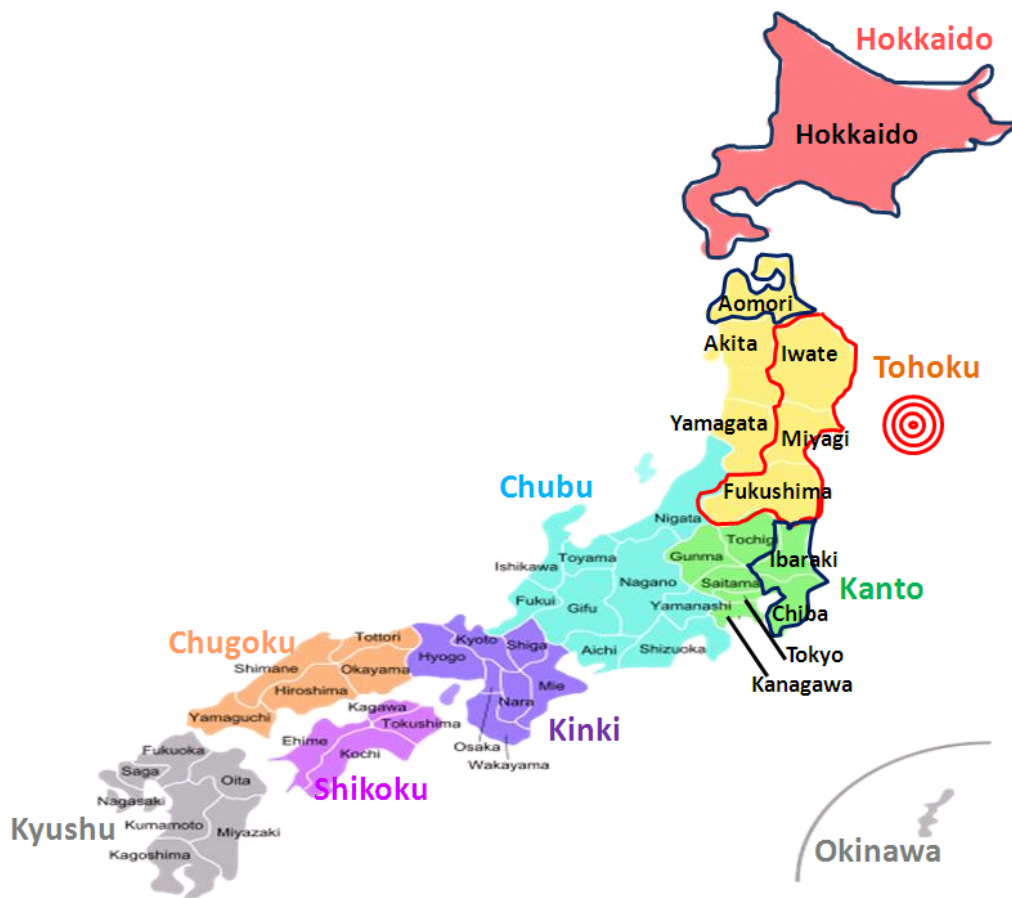


Figure 5.1: Map of 7 affected prefectures and 3 main affected prefectures due to the Great East Japan Earthquake.

The cabinet office, government of Japan defined 7 prefectures as disaster areas from this large-scale earthquake. These 7 prefectures are Iwate, Miyagi, Fukushima, Hokkaido, Aomori, Ibaraki, and Chiba[5]. However this large-scale earthquake mainly

devastated 3 main regions which are Iwate, Miyagi, and Fukushima. These are prefectures in Tohoku region. Affected prefectures are shown in area covered by blue line and red line in figure 5.1. Prefectures in red line covered area are 3 main affected prefectures in Tohoku.

The amount of damage on capital stock due to this disaster is said to be about 16-25 trillion yen in total. However about amount of 9-16 trillion yen belongs to the damage on private capital stock of 7 affected prefectures. Moreover 87.5% - 92% of this amount belongs to 3 main affected prefectures in Tohoku.

Cabinet office, Government of Japan defined 2 cases of damages due to this large-scale earthquake. These 2 cases are:

Case 1 refers to damage from the earthquake.

Case 2 refers to damage from the earthquake and consequent Tsunami.

Shinozaki et al. estimated the damage on ICT related capital stock due to the Great East Japan Earthquake in [1]. Base on definition of disaster area by Japanese cabinet office, they estimated the damage on ICT related private capital stock. Moreover they also estimated demand of investment for re-installation and demand of employment in the near future. Two cases of estimation are defined as same as what Japanese cabinet office did. The result shows that damage on ICT related capital stock costs around 2.5-4.4 trillion yen in total. Demand on an investment for re-installation of ICT related stock will be around 3.9-7.0 trillion yen. And demand of employment will be around 201,000-357,000 people.

Since there is impact on ICT related capital stock, there will also be impact on information security from the loss due to this large-scale earthquake and subsequent Tsunami in Tohoku region. And it might affect information security in other regions as well.

With this motivation, we estimate possible effect on information security due to the loss from this Great East Japan Earthquake in Tohoku.

5.1 Study on Impact from the Great East Japan Earthquake

We study the impact from the Great East Japan Earthquake based on the methodology in chapter 3 and amount of damage which the Japanese government announced in [5].

Continuing from equation 3.16, we first estimate the loss of output due to this large-scale earthquake. To remind you, equation 3.16 is expressed as follows: $\mathbb{h} \equiv \{\mathbf{I} - [\mathbf{A} - \mathbf{B}\mathbf{A}^*]\}^{-1}(\hat{\mathbf{f}} - \mathbf{B}\mathbf{f}^* + \mathbf{e})$. It refers to the value of overall *output*. Moreover, each element is represented by $h_{q,i}$.

We will apply impact due to this large-scale earthquake to this overall output and then compare the result between output from normal case and outputs with impact from the disaster.

5.2 Analysis the impact on structural interdependency

When analysis the impact from the disaster on structural interdependency, we applied ratio of damage on IT system ($R_{\bar{r}}^d$) to values of economic transaction belongs to observing region in inter-regional input-output table. Only economic transaction values of specific region which we want to simulate the impact will be applied.

The modification of the calculation is applied to change amount of intermediate values in the inter-regional input-output stated by 3.5. In this case, we use

$$\bar{z}_{q,i,r,j}(\bar{r}) \equiv \begin{cases} (1 - R_{\bar{r}}^d)z_{q,i,r,j} & \text{if } r = \bar{r} \\ z_{q,i,r,j} & \text{otherwise} \end{cases} \quad (5.1)$$

instead of $z_{q,i,r,j}$ in 3.5. Here, \bar{r} refers to region where the earthquake occur. Other calculation steps upto equation 3.16 in chapter 3 remain the same.

5.3 Additional data for the study on impact from the Great East Japan Earthquake

Beside Inter-Regional Input-Output table for 2005 : 平成 17 年地域間産業連関表 [23] and Japan Industrial Productivity Database 2008 : 日本産業生産性 (JIP) データベース (JIP Database 2008)[30], which are stated in chapter 4, following data are also required for estimating the impact from the Great East Japan Earthquake:

1. **Special cabinet meeting material on monthly economic report due to the earthquake** : 月例経済報告等に関する関係閣僚会議震災対応特別会合資料 - 東北地方太平洋沖地震のマクロ経済的影響の分析 [5]

This short special report is provided few weeks after the Great East Japan Earthquake by Cabinet office, Government of Japan. The overall loss due to this large-scale earthquake is said to be about 16-25 trillion yen (approx. 208-325 billion US dollars ¹). However 9-16 trillion yen (approx. 117-208 billion US dollars)

¹Exchange rate on Oct 19, 11 : 1USD = 76.75 yen

belongs to 7 affected prefectures. Moreover 87.5%-92% of this amount belongs to 3 main affected prefectures which locate in Tohoku.

2. Gross Capital Stock by Industry : 産業別資本ストック [4]

This dataset gives values of gross capital stock in national-level. We use the values of gross capital stock from year 2009 which is the newest at the time we estimated the impact.

For simplicity, we use value from year 2005 provided in Inter-Regional Input-Output table[23] and Japan Industrial Productivity Database 2008[30], value from year 2009 provided in Gross Capital Stock by Industry [4]. These values will be used to find variables which serve as proxies in our calculation. We will soon explain in this chapter.

5.4 Variables for impact estimation

1. Regional production ratio and Regional capital stock First we use to dataset of Inter-regional input-output table[23] and Japanese nationwide capital stock[4] to find ratio of each region's capital stock. The values of regional production value belongs to each region and nationwide production value are used. We can find both values in Inter-regional input-output table. Then we find *proxy of regional production ratio* by following equation:

$$R_P = P_r / P_{total} \quad (5.2)$$

where R_P denotes regional production ratio
 P_r denotes regional production value
 P_{total} denotes total production value of all regions

The *proxy of regional capital stock* of each region can be calculated by

$$C_r = R_P * C_n \quad (5.3)$$

where C_r denotes regional capital stock
 C_n denotes nationwide capital stock from dataset [4]

2. Regional ratio of damage Next we find a ratio between damage for the region that we want to analysis and regional capital stock in 5.3. It can be calculated by

$$R_r^d = D^{all}/C_r \quad (5.4)$$

where D^{all} denotes overall damage on capital stock from the disaster

This regional ration of damage is used to find effect from this disaster by equation 5.1.

3. The portion of IT capital stock and Damage on IT system From expression of the level of IT dependency as shown in chapter 4 equation 4.1, We apply this concept to indicate portion of IT capital stock in each sector to larger scope. Here we focus on IT portion of each region in our work, we change a concept of observing IT capital stock by industrial sector in equation 4.1 a little bit.

Change the level of IT dependency in equation 4.1 from sectoral viewpoint to overall viewpoint. Hence we use total values of IT capital stock among industries and non IT capital stock instead. Then find *proxy for ratio of IT capital stock* as follows:

$$t_{total} = IT_{total}/(IT_{total} + nIT_{total}) \quad (5.5)$$

where IT_{total} denotes total amount of IT capital stock

nIT_{total} denotes total amount of non IT capital stock

Then the ratio of IT dependency is used when estimate the impact due to damage on IT related portion in each region.

We apply ratio of IT capital stock in equation 5.5 to the amount of damage. Hence *the proxy of portion of damage on IT system* can be defined by

$$D^{IT} = D^{all}t_{total} \quad (5.6)$$

where D^{IT} is damage on IT system

D^{all} is overall damage from the disaster

5.5 Estimation of the effects from an investment in information security

To estimate effects from investment in information security, we assume that investment in IS will help reducing the damage from disaster. Here, we assume that a pre-disaster investment in information security can improve the amount of damage from the

disaster by 10%. Pre-disaster investments in information security might also include an investment in secure data center where attacker cannot access to core information system, installation of security monitoring software, or well education of IT staffs on emergency responses. An appropriate investment in information security is expected to reduce severity to the information system and keeps security control properly function during downtime.

The proxy of portion of reduced damage on IT system will be

$$\tilde{D}^{IT} = (1 - \text{degree of improvement(in \%)})D^{IT} \quad (5.7)$$

where \tilde{D}^{IT} is reduced amount of damage on IT system
 D^{IT} is damage on IT system in 5.6

After adjusting the value of damage, our ratio of damage on IT system (R_{τ}^d) will be recalculated. We define (\tilde{R}_{τ}^d) as the *ratio of damage on IT system with improvement on damage* as follows:

$$\tilde{R}_{\tau}^d = \tilde{D}^{IT} / c_r \quad (5.8)$$

Replace R_{τ}^d in equation 5.1 by \tilde{R}_{τ}^d to calculate the impact from disaster when there is an improvement on damage due to investment in information security.

We use the same absolute value of \tilde{D}^{IT} in the simulation for any region when we study for an advantage of investment in information security.

Moreover we also estimate impact on interdependency of information security due to the Great East Japan Earthquake by using the same methodology as in chapter 3. The impact from this earthquake is applied to inter-regional input-output table as mentioned in equation 5.1. Hence we will be able to observe differences between interdependency of information security *with and without* impact from the large-scale earthquake.

Chapter 6 Results and discussion on Interdependency of Information Security from the Empirical Study

Here we start from sectoral and regional interdependency of information security. In our study, we collect result based on dataset with 12 industrial sectors. The results from our analysis show values of interdependencies between pairs of regions and sectors. The values of information security backward dependency or ISBD (shown in %) are arranged in descending order.

Dataset with 53 industrial sectors is used to consider more about interdependency of information security in Agriculture (sector 01) and Financial, insurance, and real estate (sector 10). We need to observe more detail on interdependency of information security for these 2 industrial sectors because the results for these sectors show very low value of information security backward dependency (or ISBD) which we use to find characteristics for each industrial sector and region. Hence we cannot observe any characteristic for these 2 industrial sectors by using dataset with 12 industrial sectors.

After that we show result with impact from the Great East Japan Earthquake. Due to the government's announcement about damage from the Great Japan Earthquake in chapter 5, we set 4 testing scenarios which are:

- Case 1 Full damage from the earthquake.
 Amount of 9 trillion yen is used as damage value for this case.
- Case 2 Damage from the earthquake with some reduction due to investment in information security.
 Amount of 9 trillion yen with 10% reduction is used as damage value for this case.
- Case 3 Full damage from the earthquake and consequent Tsunami.
 Amount of 16 trillion yen is used as damage value for this case.
- Case 4 Damage from the earthquake with some reduction due to investment in information security.
 Amount of 16 trillion yen with 10% reduction is used as damage value for this case.

These 4 cases are applied as a scenarios if the earthquake introduce the same amount of damage in Tohoku and Kanto. We also try to simulate impact if there is the same amount of damage occur in Kanto because

- 1.) In economic perspective, Kanto is a region which has the largest economic scale.
- 2.) Information security in Kanto shows high influence to other regions. We will show this point later in section 6.1.2.
- 3.) There are 70% prediction that there might be a large-scale earthquake in Kanto within 4 years (due to the latest news in early 2012).

After that we first observe the change in output due to the damages in 4 cases as above. First we observe the order of the same combination between region and sector as well as its difference of absolute value of output.

Then we test to find some changes in interdependency of information security. We set the scenarios if the same amount of damage occurs in Tohoku and Kanto. Then observe changes in 3 regions which are Tohoku, Kanto, and Kyushu due to some reasons. We choose Tohoku, because it is a region where the Great East Japan Earthquake is exactly occur. Hence we would like to estimate the changes due to damage in this region. Next we choose Kanto as stated above. Finally, we choose Kyushu because it is region where we can observe changes on absolute value of output due to impact from the damage. We will show this point later in section 6.2.

6.1 Sectoral and regional interdependency of information security

The values of interdependency of information security show interconnectedness between 2 pairs of regions and industrial sectors. To analyze the result, we first set the same threshold at $ISBD = 0.01\%$ for all industrial sectors and regions. From our primary analysis we found that, in our case, we can get information about characteristics of interdependency of information security when we set threshold at $ISBD = 0.01\%$. After that we analyze to find some characteristics of each region and industrial sector. By this, we count number of dependent supply-side region-sector pairs, which their value of $ISBD$ is at least equal the value of the threshold. Then find regional and sectoral interdependencies of information security.

The term of supply-side sector or supply-side region are used to indicate the sector or region in output-side perspective (producer). The supply-side group provides products or services as output according to demand from demand-side group.

On the other hands, demand-side sector or demand-side region are used to indicate

the sector or region in input-side perspective (purchaser). The demand-side group receives products or services as input according to its demand from supply-side group. The interdependency which we test will tell that how much do firms in demand-side group depend on supply-side group.

The combination between region and industrial sector is called *group*. If region and industrial sector which are combined come from *demand-side*, we call it as *demand-side group*. In contrast, if region and industrial sector which are combines comes from *supply-side*, we call it as *supply-side group*.

6.1.1 Sectoral interdependency of information security

In sectoral perspective, we observe interdependency of information security between demand-side groups and supply-side groups by sector. First, we would like to list up some characteristics and interesting points which can be observed from the result are listed by industrial sector. The listed results will be used in our discussion for sectoral and regional interdependency of information security afterwards.

1. Sector 01 - Agriculture

The result of agriculture shows very low value of ISBD. From our raw data, the result shows that the values of ISBD belong to this industrial sector is about 10-time lower than the value of ISBD at the threshold. Table A.2 in appendix A shows that there is no dependent supply-side sector in any supply-side region which demand-side agriculture show interdependency when tested.

We move to a larger dataset with number of industrial sector equal to 53 industrial sectors to find more characteristic. The result from this larger dataset also shows very low values of ISBD as same as when we analyze from dataset with 12 industrial sectors.

One reason is that they did not divide data belongs to this industrial sector into some smaller sectors in dataset with 53 industrial sectors. However from the result we think that the results are not much surprise since activities in industrial sector of agriculture seems not to relate to information security much.

2. Sector 02 - Mining

From result in table A.3, we can see that demand-side sector of mining in all supply-side regions show high interdependency when tested with dependent supply-side sectors of other manufacturing(06), commerce & logistic(09), and services(12). This means demand-side sector of mining is likely influenced by

these 3 supply-side sectors. These are the supply-side sectors which might receive high effect from demand-side sector of mining in all regions if there is any incident regarding information security in the demand-side sector of mining in any region.

In addition, from the result with raw data, we found that the highest percentage of the value of ISBD is presented when we tested the demand-side sector of mining in each region with supply-side sector of services(12) in its own region.

3. Sector 03 - Food and Beverage

From result in table A.4, we can see that demand-side sector of food & beverage in all regions show high IS interdependency when tested with dependent supply-side sectors of food & beverage, which is its own region, other manufacturing(06), and commerce & logistic(09). On the other hands, demand-side sector of food & beverage in all regions show no interdependency when tested with supply-side sector of mining (02), machinery (05), and construction (07). One of the reasons might be related to activities inside these industrial sectors which might not highly related to sectors of food & beverage

4. Sector 04 - Metal

Demand-side sector of metal in all regions highly depend on firms in sector of metal(04), its own sector. Followed by sector of other manufacturing(06), and commerce & logistic(09). This can be inferred that information security in sectors of metal is likely have interconnection in term of information security between firms in its own sectors regardless regional influence. We can observe such information from our raw data that top 5 supply-side groups, which show high interdependency (with high value of ISBD (%)) or high influence when tested, belongs to sector of metal in different regions. The result in this perspective can be observed by using table A.5

On the other hands, demand-side sector of metal in all regions show no interdependency when tested with sector of agriculture(01), mining(02), food & beverage(03), and machinery(05). Hence these might be industrial sectors which are insensitive due to information security incident in demand-side sector of metal.

5. Sector 05 - Machinery

Result in table A.6 shows that demand-side sector of machinery in all regions show high interdependency when tested with supply-side of its own sector. Hence incident regarding information security in demand-side sector of machinery is expected to give high effect in sectoral perspective.

Other two industrial sectors which demand-side sector of machinery highly depends on are sector of other manufacturing(06) and sector of metal(04) according to the result.

In addition, when we consider our raw data of the result, we found the top 5 with the highest value of ISBD (%) always contain supply-side groups of machinery in Kanto and Chubu (C-05 and D-05). Such information gives us important characteristics that the sector of machinery in Kanto and Chubu plays an important role in terms of sectoral interdependency of information security for the sector of machinery.

6. Sector 06 - Other Manufacturing

Demand-side sector of other manufacturing shows the highest interdependency when tested with supply-side of its own sector in all regions. The total number of 56 dependent supply-side groups which are belonged to the supply-side sector of other manufacturing in table A.7 significantly shows this point. Although the sector of commerce & logistic(09) is the sector which its number of interdependent supply-side groups comes in a second place but the number of supply-side groups is less than half of the number of supply-side sector when tested with sector of other manufacturing. Such information gives us a clear idea that the sector of other manufacturing will likely affect firms in the same group of industry.

7. Sector 07 - Construction

The demand-side sector of construction shows high interdependency when tested with supply-side sector of metal(04) in all regions. One reason for such interdependency might come from activities inside each sector which relate to each other between sectors. Such interconnection between industrial sectors are unsurprising. In addition to sector of metal(04), industrial sector of construction also shows quite high interdependency of information security when tested with supply-side group from sector of other manufacturing(06) according to result in table A.8.

8. Sector 08 - Utilities

According to the results in table A.9, demand-side sector of utilities in all regions show the highest interdependency when tested with supply-side groups from sector of other manufacturing(06), services(12), and commerce & logistic(09), respectively.

Carefully look for more detail in the table A.9, demand-side sector of utilities in all regions show no interdependency when tested with supply-side sector of

agriculture(01), mining(02), food & beverage(03), metal(04), and machinery(05).

9. Sector 09 - Commerce and Logistic

For demand-side sector of commerce & logistic in table A.10, the largest total of number of dependent supply-side regions is shown when tested with supply-side groups from sector of other manufacturing(06), services(12), and ICT(11). Moreover the demand-side sector of commerce & logistic also shows high interdependency to its own sector as well.

In contrast, demand-side sector of commerce & logistic shows no interdependency when tested with supply-side sector of agriculture(01), mining(02), food & beverage(03), and metal(04).

10. Sector 10 - Financial, Insurance, and Real Estate

The result for demand-side sector of financial, insurance, and real estate shows very low value of ISBD when tested for interdependency with all supply-side groups. The only 1 supply-side group that shows the interdependency is supply-side sector of services(12) in Kanto(C) region as shown in table A.11. That is because our raw data shows that the value of ISBD in this demand-side sector is about 10 times lower than the value of ISBD at the threshold.

Although the number of dependent supply-side sectors is as same as when we tested for sector of agriculture(01) but there is some differences between these 2 industrial sectors. In addition, the use of dataset with 53 industrial sectors help showing some differences as well as factors which make the value of ISBD becomes low.

Sector of financial, insurance, and real estate in dataset with 12 insuatrial sectors is divided into 3 sub-industrial sectors as follows:

12 industrial sectors		53 industrial sectors	
Sector ID	Sector name	Sector ID	Sector name
10	Financial, Insurance, and Real Estate	0400	Financial and
			Insurance
		0410	Real Estate
		0420	Rental housing

Tested result of interdependency of information security for sector 0410 and 0420 show no interdependency when tested. For sub-sector of financial and insurance(0400), the result can be shown as in table A.14. In this table, we only show result for some dependent supply-side sectors which show interdependency when

tested with demand-side sectors of financial and insurance(0400). There is no interdependency between demand-side sectors of financial and insurance(0400) and other remaining supply-side sectors. So the result between those industrial sectors become all zero.

Demand-side sub-sector of financial and insurance(0400) shows very high interdependency when tested with supply-side groups from sub-sectors (0090) which belong to sector of other manufacturing(06), sub-sectors (0400) which belong to sector of financial, insurance, and real estate(10), sub-sectors (0440 and 0450) which belong to sector of ICT(11) and sub-sectors (0490, 0500, and 0510) which belong to sector of services(12).

11. Sector 11 - ICT

The sectoral perspective for demand-side sector of ICT shows the highest interdependency when tested with supply-side groups from other manufacturing(06), commerce & logistic(09), services(12), and supply-side groups from its own sector.

However, demand-side of ICT does not show any interdependency of information security when tested with supply-side groups from agriculture(01), mining(02), food & beverage (03), metal(04), and machinery(05). Such result can be observed from table A.12.

12. Sector 12 - Services

From table A.13, the demand-side sector of services in all regions show the highest interdependency when tested with supply-side sector of other manufacturing(06). Followed by supply-side sector of commerce & logistic(09) and supply-side sector of machinery(05).

The only supply-side sectors which demand-side sector of services regardless region show no interdependency when tested is the supply-side sector of mining(02). That means supply-side sector of mining(02) is the only industrial sector which gives no influence to demand-side sector of services. Moreover the supply-side sector of mining will likely be least affected if there is any incident regarding information security.

6.1.2 Regional interdependency of information security

In regional perspective, we observe interdependency between demand-side industrial sectors in each region and all dependent supply-side industrial sectors in each supply-side region.

The total number of dependent supply-side regions and dependent supply-side sectors by each region are shown in table A.16. in appendix A.

First, let look at the dependent supply-side region. From table A.16 we can see that interdependency of information security in each region likely shows when tested with industrial sectors inside its own region and industrial sectors in Kanto(C).

Consider from demand-side perspective, Kanto(C) shows that it is *the most influential* region in term of information security from demand-side perspective. That is because information security in many demand-side regions highly rely on supply-side of Kanto(C). On the other hand, Shikoku(G) and Okinawa(I) , which are 2 smallest economic scale region as shown in table 4.3, rely on large number of supply-side groups across Japan. These 2 regions becomes *the most influenced* regions in demand-side perspective. That is because information security in these 2 regions is influenced by large number of supply-side groups.

The ratio between number of dependent supply-side regions which is the same as demand-side region and number of dependent supply-side region which is not the same as demand-side region is shown in table 6.1. Values in this table come from the ratio between number in column *Total(Self)* and *Total(Exclude)* in table A.16.

Demand-side region (Region ID)									
A	B	C	D	E	F	G	H	I	Total
0.663	0.618	1.302	0.625	0.784	0.568	0.445	0.607	0.532	0.642

Table 6.1: Ratio between dependent supply-side regions which is the same as demand-side region and number of dependent supply-side region from other regions.

We can see that interdependency of information security belongs to Kanto(C) show high value of ratio which mean interdependency of information security is concentrate inside its own region.

Shikoku(G) has the smallest value. This means that information security in Shikoku(G) has high interdependency with industrial sectors in other regions. Information security of Shikoku(G) is then influenced by high number of supply-side groups and make this region become *the most influenced* region as a result.

6.1.3 Discussion

From the result, the summary table for sectoral interdependency can be presented as in table 6.2.

Demand-side sector name (ID)	Sector ID of supply-side sector (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Agriculture(01)	×	×	×	×	×	×	×	×	×	×	×	×
Mining(02)	×	×	×		×		×					
Food&beverage(03)		×			×		×					
Metal(04)	×	×	×		×							
Machinery(05)	×	×	×									
Other manufacturing(06)	×		×		×							
Construction(07)	×	×	×				×					
Utilities(08)	×	×	×	×	×							
Commerce&logistic(09)	×	×	×	×								
Financial, insurance, and real estate(10)	×	×	×	×	×	×	×	×	×	×	×	
ICT(11)	×	×	×	×	×							
Services(12)		×										

Table 6.2: Summary of sectoral interdependency of information security

From table 6.2, each symbol indicate level of interdependency of information security which we can observe from the result. The sign “ ” represents the case that number of dependent supply-side group is at least 50% of the highest value of each industrial sector. “ ” represents the case that there is number of dependent supply-side group but lower that 50% of the highest value of each industrial sector. “ ” represents the case that there is number of dependent supply-side group but not exceed 10% of the highest value of each industrial sector. “×” represents the case that there is no dependent supply-side group when tested for an interdependency.

By using *result along column* in table 6.2, we firstly find dependent supply-side industrial sectors which show high influence. These are industrial sectors which are *highly depended by* demand-side industrial sectors. In another word, they are industrial sectors in the group of *influential* industrial sectors in term of information security. An important of this group of industrial sectors is that industrial sectors belong to this group might easily be affected by incident regarding information security which occur in demand-side groups. In another word, we might be able to call this group of industrial sector as *critical sectors* in term of information security.

Information security of industrial sectors in the group of the most influential industrial sectors are depended by high number of demand-side groups. Critical sectors which can be observed from table 6.2 are

- 1.) Other manufacturing(06)
- 2.) Commerce and logistic(09)
- 3.) Services(12)

On the other hand, following industrial sectors have characteristics, which can be referred as *the least influential* industrial sectors in term of information security, are

- 1.) Agriculture(01)
- 2.) Mining(02)
- 3.) Food and beverage(03)

A main reason why these industrial sectors become the least influential sectors because demand-side industrial sectors are not rely of this group of industrial sector much. However if we consider number of dependent supply-side sector of construction(07) in table A.15, we will also see that the number of dependency supply-side sector is very low. So we also include sector of construction as another industrial sector in the group of the least influential sector in term of information security. Moreover, there are some additional reasons why these 4 industrial sectors are listed in the group of the least influential industrial sector.

First, if we consider level of IT dependency, IS measure, and Security risk level in chapter 4, we will be able to see that these values which belong to sector of agriculture(01), mining(02) and construction(07) go towards low level.

Second, for the case of sector of food and beverage(03), its production values which refer to economic activities is not high. Another reason is likely related to activities of this industrial sector. If we consider table 6.2, we can see that interdependency is shown when supply-side sector of food and beverage(03) is tested by demand-side industrial sector of services(12) and its own sector. This are reasons why these 4 industrial sectors do not show significant interconnection in term of information security.

Other industrial sectors which are not belong to these 2 groups can be called as a *moderate influential* industrial sectors.

Next we observe significant characteristics of demand-side industrial sectors. To do so, we observe the *result in each row* in table 6.2. There are 5 main groups industrial sectors divided by their main characteristics.

1. Industrial sectors which their interdependency of information security is highly shown *only* when tested with supply-side sector of critical industrial sectors.

There are 2 demand-side industrial sectors which show such characteristic. These 2 industrial sectors are

- 1.) Mining(02)
- 2.) Utilities(08)

In this group, incident regarding information security which occur in demand-side of this group of industrial sectors will likely affect main critical sectors more than other sectors. An investment in information security in such group of industrial sector might help reducing effect and risk that would harm critical sectors.

2. Industrial sectors which their interdependency of information security is highly shown when tested with supply-side of its own sector and *all* critical industrial sectors.

There are 5 industrial sectors which have such characteristics. They are

- 1.) Food and beverage(03)
- 2.) Machinery(05)
- 3.) Commerce and logistic(09)
- 4.) ICT(11)
- 5.) Services(12)

As we can see, this group of industrial sector also includes some critical industrial sectors.

Information security incident in demand-side of this group of industrial sector not only harm information security system inside its own region. In contrast, they have high possibility that this group of industrial sectors might harm many industrial sectors beside critical sectors. Significant characteristic which belongs to this group of industrial sector is that they depends on high number of supply-side industrial sectors. Therefore information security incident might lead to larger scope of effect in sectoral perspective.

In addition, if we consider total value of dependent supply-side sector which is belong to demand-side sector of machinery(05) and services(12) in the most right column in table A.15, these 2 sectors have the largest value in this column. This largest values of total number of dependent supply-side sector also reveal that sector of machinery(05) and services(12) are *the most influenced* industrial sectors in demand-side perspective. Hence their information security is highly influenced by many supply-side groups.

An investment in information security in such group of industrial sector would help reducing risks which might occur as an effect from security incident in a wider scope comparing with investment in information security in other groups.

3. Industrial sectors which their interdependency of information security is highly shown when tested with supply-side of its own sector and *some* critical industrial

sectors.

From table A.15, there are 2 industrial sectors which we can judge as members in this group. They are

- 1.) Metal(04)
- 2.) Other manufacturing(06)

Quite similar to the upper group, information security incident which occurs in this group of industrial sector with not only harm its own sector but also other supply-side industrial sectors which are in critical sectors. However, the scope of effect is likely be smaller and only some critical structure are likely be affected. That is because this group of demand-side industrial sector depends on lower number of supply-side industrial sectors.

4. Industrial sectors which do not show or rarely show interdependency of information security when tested with supply-side industrial sectors.

When using dataset with 12 industrial sectors, demand-side sectors which belong to this group are

- 1.) Agriculture(01)
- 2.) Financial, insurance, and real estate(10)

An investment in information security in this group of industrial sector might not show high effectiveness. That is because demand-side industrial sectors in this group do not show high interdependency in term of information security. Such characteristic also means that industrial sectors in this group might not have high significant in term of information security.

However, for the case of demand-side sector of financial, insurance, and real estate(10), such characteristic is shown due to influence from demand-side sub-sectors of real estate(0410) and rental housing(0420) in dataset with 53 industrial sectors. So that we must treat sub-industrial sector of financial and insurance(0400) separately from this demand-side group.

By using dataset with 53 industrial sectors, the sub-industrial sector of financial and insurance(0400) shows high interdependency of information security when tested with supply-side sub-industrial sectors which belong to other manufacturing(06), financial, insurance, and real estate(10), ICT(11), and services(12). Therefore we might consider demand-side sector of financial, insurance, and real estate(10) or its sub-industrial sector of financial and insurance(0400) as demand-side sector with characteristics as mentioned in group 3. This might be more suitable for this demand-side industrial sector.

5. Industrial sector which show no interdependency of information security when tested with supply-side of its own industrial sector.

Based on dataset with 12 industrial sectors, there is only 1 industrial sector which does not belong to any group from 1 to 4. That is industrial sector of construction(07).

Although if you consider the result shown in table 6.2, demand-side industrial sector of mining(02) also show no interdependency of information security when tested with supply-side of its own industrial sector. However we think that its characteristic as in group 1 is more important.

Now look at the result from regional perspective.

Demand-side region name (ID)	Region ID of supply-side region (Region ID)								
	A	B	C	D	E	F	G	H	I
Hokkaido(A)									×
Tohoku(B)							×		×
Kanto(C)									×
Chubu(D)									×
Kinki(E)									×
Chugoku(F)	×								×
Shikoku(G)	×								×
Kyushu(H)	×								×
Okinawa(I)									

Table 6.3: Summary of regional interdependency of information security

First consider each column in table 6.3. We can see that information security in all demand-side regions highly depend on information security in Kanto(C). This make supply-side groups in Kanto(C) becomes *the most influential* region in term of information security. Moreover such region could have high possibility of being affected by information security incidents. Although its economic scale and interdependency of information security inside its own region are high, but with high interconnection and transactions with other regions this group of region becomes critical in term of information security.

On the other hand, supply-sides groups belongs to Okinawa(I) show no interdependency when tested by demand-side sectors in all regions except its own region.

Hence Okinawa(I) becomes *the least influential* region in term of information security. In addition to this point, supply-side groups in regions such as Shikoku(G), Hokkaido(A), and Tohoku(B) are regions where their information security does not show high influence to demand-side regions.

If we consider from an influential of supply-side regions, one factor which shows some relation would be their *economic scale*. That is if economic scale of the region is large, they would have high economic activities and higher need of investment in information security in order to reduce its possibility of being affected.

Next consider the each row in the same table, we can see that demand-side regions with small economic scale show their necessity of relying on supply-side regions. According to regional economic scale in table 4.3, information security in small economic scale regions such as Okinawa(I) and Shikoku(G) seems to be influenced by larger number of supply-side regions. We call such group of demand-side regions as *the most influenced* region. Especially, demand-side region of Shikoku(G) where information security is influenced by all supply-side regions. So we can call Shikoku(G) as *the most influenced* region in term of information security. However result for Hokkai do does not show the same in the same trend.

Extremely large economic scale regions of Kanto(C) in the demand-side perspective, in contrast, depend on smaller number of supply-side regions. However the trend is not also be the same. That is because when consider second and third most influenced demand-side regions, Tokoku(B) and Hokkaido(A) comes respectively.

From what we can observe in regional perspective, the economic scale is one of the main factors which make each region becomes the most/least influential.

For the case of the most/least influenced region, economic scale shows influence when consider interdependency of information security between firms inside each region. That is interdependency of information security of region with large economic scale usually shows when tested with sectors inside its own region. This can be observed from absolute values in column *Total(Self)* in table A.16. For this case, one main characteristic of interdependency of information security in regional perspective is that *the demand-side of each region highly shows interdependency of information security when tested with supply-side of Kanto(C) and its own region*.

6.2 Impact from the Great East Japan Earthquake on information security

6.2.1 Result of changes on output

1. Result of changes when there is damage in Tohoku

In our estimated result for Tohoku(B), we found that impact from disaster likely affects output of some industrial sectors in Tohoku(B) as well as Kyushu(H) and Hokkaido(A).

From our observation, we found that the value of output between industrial sectors in Tohoku(B) and some industrial sectors in Tohoku(B), Kyushu(H), and Hokkaido(A) reduced so the their order of output are changed when there is damage on IT-related capital stock from disaster. However Tohoku(B) is the most affected region.

From sectoral perspective for Tohoku(B), industrial sectors which seem to be affected most is sector of other manufacturing(06). Actually, this sector is one of critical industrial sectors as shown in section 6.1 ¹. We found that following industrial sectors are sectors which are affected by this damage: services(12), financial, insurance, and real estate(10), food & beverage(03), agriculture(01), and mining(02). Anyway the changes in output of these industrial sectors mostly occur with firms in Tohoku(B). Only industrial sector of other manufacturing(06) in Kyushu(H) and agriculture(01) in Hokkaido(A) are affected when there is damage in Tohoku(B).

10% reduction in damage from investment in IS helps improving amounts of value of outputs. For case 1 in Tohoku(B), a summation of value of output is increased by approximately 40.8 billion yen. when we assume that investment in IS helps reducing damage for 10%. And for case 2 in Tohoku(B), a summation of value of output is increased by approximately 68.3 billion yen. Although damage in case 2 is about 1.78 times larger than damage in case 1 but the results show that 10% of reduction in damage due to investment in information security makes difference between value of outputs belong to case 2 becomes approximately 3.4 times higher than case 1 ².

¹To remind you, we found that there are 3 critical sectors which might be highly affected when there is any IS incident. These 3 sectors are other manufacturing(06), commerce&logistic(09), and services(12)

²We observed by comparing value of output with full damage and value of output with 10% reduction in damage due to investment in information security.

2. Result of changes when there is damage in Kanto

We applied the same amount of damage on IT-related capital stock from this disaster to Kanto(C) and simulate the possible result. First we observe the change in output due to damage in Kanto(C). We found that with the same amount of damage which occur in Tohoku(B), our simulated results show lower level of possible effect for Kanto(C). This mean the same amount of loss regarding IT-related capital stock will affect less if it happen in Kanto(C). One reason which might support such result is that the amount of damage is small comparing to economic scale of Kanto(C).

When using the same amount of damage, value of regional ratio of damage for Tohoku(B) and Kanto(C) are shown in table 6.4.

	Tohoku	Kanto
Case 1 full damage	12.27%	1.71%
Case 1 with 10% reduction in damage	12.17%	1.69%
Case 2 full damage	21.82%	3.03%
Case 2 with 10% reduction in damage	21.64%	3.01%

Table 6.4: Regional ratio of damage in percentage.

Similarly to the estimated results for Tohoku(B), sector of other manufacturing(06) shows that it is likely to be affected when there is loss in Kanto(C)'s IT-related capital stock. That is because values of output for sector of other manufacturing(06) in Kyushu(H) and Tohoku(B) are reduced and their order according to the absolute value of output are changed. Moreover, sector of other manufacturing(06) shows high influence on information security for Kanto(C) as shown in section 6.1. That means, sector of other manufacturing(06) is likely to be affected, in other word sensitive, due to incident regarding information security. Anyway, it seems that the impact will be visible when we simulate the impact from damage case 2 (impact from earthquake and tsunami). However industrial sector of mining(02) in Hokkaido(A) is another group which is affected by the damage in case 2.

For simulation with damage in case 1 (impact only from earthquake), we found that there is no change with the same amount of damage that occurred in Tohoku(B).

Moreover 10% reduction in damage from investment in information security helps improving amounts of value of outputs in quite similar ratio. For case

1 in Kanto(C), a summation of value of output is increased by approximately 46.1 billion yen when we assume that investment in information security helps reducing damage for 10%. And for case 2 in Kanto(C), a summation of value of output is increased by approximately 80.6 billion yen (approximately 3.5 times higher than case 1).

6.2.2 Result of changes on interdependency of information security

Here we observe reduction of interdependency of information security in some regions which are Tohoku(B), Kanto(C), and Kyushu(H). We did not observe reduction of interdependency of information security in Hokkaido(A) because the industrial sectors in Hokkaido(A) which are affected by the damage have quite low absolute value of output. In addition, in information security perspective, information security in Hokkaido does not show high influence to industrial sectors in other regions.

1. Result of changes when there is damage in Tohoku

According to our result when there is damage in Tohoku, in both cases when firstly observe results in Tohoku region. Table B.1 and B.2 in appendix B show number or missing supply-side groups when we tested for interdependency of information security between industrial sectors in Tohoku(B) and supply-side sectors and regions, respectively. We found that the reduction of interdependency of information security is concentrated between industrial sectors inside Tohoku(B) and between industrial sectors in Tohoku(B) and Kanto(C) when we consider from a demand-side perspective.

The reduction of interdependency usually occur with industrial sector of financial, insurance, and real estate(10) other manufacturing(06), services(12), and commerce and logistic(09)

But when we move to observe the reduction of interdependency in Kanto(C) and Kyushu(H) due to the lost from damage in Tohoku(B), we found that there is very little effect from the damage in Tohoku(B). The result can be seen in table B.3–B.4 for Kanto(C) and table B.5–B.6 for Kyushu(H), respectively.

2. Result of changes when there is damage in Kanto

But when the same damage occur in Kanto(C), we found that there would be a smaller reduction of interdependency of information security if we consider from a demand-side perspective.

When there is damage in Kanto(C), Tohoku(B) shows some reduction of interdependency of information security when tested but at a low level. The results are shown in table B.7–B.8.

The reduction of interdependency of information security can be easily observed in Kanto(C). From the results in table B.9–B.10 we can see that the reduction is likely be between industrial sectors inside Kanto(C) due to the fact that information security of industrial sectors in Kanto(C) highly rely on each other inside region as shown in section 6.1. The reduction of interdependency of information security is likely to be in industrial sectors of services(12) and commerce and logistic(09).

But when we observe the reduction of interdependency of information security in Kyushu(H) the results show that Kyushu(H) barely shows the reduction of interdependency of information security when tested. See table B.11–B.12 for detail. The number of missing supply-side groups only shows in case 2 of damages.

6.2.3 Discussion

Our estimation shows that the effect from the Great East Japan Earthquake on IT-related capital stock is likely limited in some regions and some industrial sectors. Especially results from sectoral perspective that show the limited scope of effect. The result also emphasize that 3 critical industrial sectors in term of information security, which stated in discussion part of section 6.1, would be easily affected.

From this estimation, supply-side industrial sector of other manufacturing(06), which is one of critical sectors, seems to be the most affected industrial sector due to the loss on IT-related capital stock from the disaster.

When apply the same amount of damage on IT-related capital stock to both Tohoku(B) and Kanto(C), we found that degree of effect on Tohoku(B) is higher than Kanto(C). That might be because the amount of damage on IT-related capital stock is quite low when compare with production value of Kanto(C).

We can infer from such results that pre-disaster investment in information security should be done, especially in some critical industrial sectors as well as some locations where they usually be affected. Moreover proper investment in information security might help reducing severity of the impact when disaster occurs.

According to the result, investment strategies for some regions and some sensitive sectors can be implied from this study. First, the result can confirm that critical sectors which we stated in section 6.1 are sensitive to incidents regarding information security. When we test the impact on interdependency of information security, the

reductions of interdependency of information security are shown for this industrial sectors. Such reduction of interdependency of information security can also refer to sensitivity of information security in that industrial sector or region.

Second, the result shows that when there is lost on information security of a specific area, the effect on interdependency of information security likely shown the same trend as affected region's characteristics. For example: when we tested for the change of interdependency of information security due to the lost in Tohoku, the reduction of interdependency of information security highly occur with supply-side industrial sectors in Tohoku and Kanto. This is the same as when we found in section 6.1.

Third, affected supply-side industrial sector might be different by region. For example: when the damage occur in Tohoku(B), in addition on critical sectors which are likely affected by the lost in demand-side sectors in Tohoku(B), supply-side sector of financial, insurance, and real estate(10) also shows high reduction of interdependency of information security. Hence this sector should also be considered by the investor of information security systems.

However there are some additional interesting point which can be study more in this part of our work.

The first point is that we used the same absolute amount of damage in order to simulate the impact if the damage occur in Kanto(C). According to the economic scale or production value of Kanto(C) and the absolute amount of damage, the size of absolute amount of damage is small comparing to Kanto's economic scale. Rather than the absolute amount of damage, we might apply ratio of the damage for the simulation.

The second point is about the amount of damage itself. Here we refer to the amount of overall damage which Japanese government announced a few weeks after the Great East Japan Earthquake. From this point, we might apply amount of damage which belongs to each industrial sector. However more data are required to this point of study.

Chapter 7 Conclusion

In this paper, we have presented our study on empirical results about sectoral and regional interdependency of information security from demand-side perspective. We use the results from demand-side perspective to list characteristics of each industrial sector and region. Moreover we also group the similar industrial sectors or regions together so that the reader can find some similarities between them.

We discussed about characteristics of interdependency of information security at the end of each section from demand-side perspective in chapter 6. From the discussion, we can expect similar investment strategy for regions or sectors which belong to the same group due to their characteristics.

First, we observed dependent supply-side industrial sectors which are depended by demand-side industrial sectors. According to our results, we pointed out 3 main supply-side industrial sectors as critical sectors. Information security of critical sectors are highly depended by information security of the demand-side industrial sectors. On the other hand, we also pointed out the least influential sectors which are supply-side industrial sectors which their information security are depended by small number of demand-side industrial sectors.

Next, we observed demand-side industrial sectors and regions about how do they are influenced in term of information security. The most influenced demand-side industrial sectors or regions play an important role. That is because this groups of demand-side industrial sectors or regions depend on high number of supply-side groups. As a result, if there is incident regarding information security in this group of demand-side industrial sector or region, there would be high impact due to some the lost on information security system.

After discussion in sectoral perspective, we move to discussed in regional perspective in order to find the most/least influential region as well as the most/least influenced region.

After that a study on the impact due to the lost from the Great East Japan Earthquake on March, 2011 helps us understand more about the characteristic of interdependency of information security. We estimated the lost and changes due to this large scale disaster to see the impact which might occur in some regions. The estimation result support our results in the first part since reduction of interdependency of information security shows when tested with supply-side groups from the groups of critical

sectors. Moreover their affected supply-side regions also support our assumption in the first part as well.

In sectoral perspective, the level of IT dependency and IS measures show high influence due to our result. Moreover if we carefully consider industrial sectors which show interdependency of information security when tested by each demand-side industrial sector, we could see that activities inside each industrial sector also influence. That is we usually see interdependency when tested between industrial sectors which their activities are related.

In order to reduce possibility of effect on critical industrial sectors, investor of the information security demand-side sectors belong to group 1 and group 2 discussed in section 6.1.3 chapter 6 should consider more on their investment in information security. That is because demand-side industrial sectors in group 1 and 2 are highly rely on information security in critical industrial sectors. However critical sectors also have to consider in order to maintain their security as well.

According to our result industrial sectors belong to group 2 and 3 should consider their investment in information security by considering regional influence. The main reason is that industrial sectors in these group highly show interdependency when tested with its own sector. Hence when incident regarding information security occurs in such groups, they could have higher possibility that the effect would spread within the same industrial sectors in many regions.

In regional perspective, each region's economic scale shows high influence when we consider *influential supply-side region*. The larger economic scale, the more demand-side groups would rely on these supply-side regions. Moreover these would be easily affected regions if any information security incident occur.

According to our result, investor of the information security should consider more on *moderate influenced regions with high number of dependent supply-side from other regions*. Which regions are Chugoku(F), Kyushu(H), Chubu(D), respectively. There are some reasons why these regions would be well considered. The first reason is that these are less sensitive regions in term of information security. Lower number of dependent supply-side regions which they depend on would mean that their information security would be affected by lower possibility. The second reason is that there are existing interconnections between firms in different regions. The exist of interdependency of information security when tested between demand-side groups and supply-side groups can also be referred that there are some level of interconnection as well as activities or transactions between them. Moreover it also means that such interconnection somehow shows importance in their system. So beside an investment in information security, investor might not need to increase their investment in IT

system. The last main reason is that these 3 regions are also be members of moderate influential regions. Which means their information security would be less affected comparing to regions which are in high influential group.

However if we consider from our study on the impact from the Great East Japan Earthquake, the effect surely occur in critical industrial sectors as we expected. However if we consider more about group of demand-side sectors which reduction in interdependency of information security is shown, the group of incident sensitive demand-side sectors are in group 2 and 3. Apart from interconnections with supply-side sectors in critical group, these are demand-side industrials sectors which show high interdependency of information security when tested with their own industrial sectors. Especially when we consider from the result, the impact on information security is shown between demand-side sectors in the region where incident occur and supply-side sectors in the regions according to demand-side region's regional characteristic. We can see that reduction of information security shows between regions which have high interconnection due to regional characteristic. Especially industrial sectors which show high interdependency of information security when tested with supply-side of its own sector.

We could see that the understanding from such empirical study will help firms or government agents understand more about the nature of interdependency of information security in the country. Investors of the information security system will be able to concern more on security sensitive sectors or regions. Moreover appropriate budget allocation can be well designed according to the needs of each group of industrial sector or region. This also means that investors can effectively plan how to use their budget on information security by using the same amount or smaller amount of budget.

Acknowledgements

First of all, I would like to express my deep gratitude to my supervisor, Associate Professor Kanta Matsuura, for welcoming me as his laboratory member. I have learned a lot from him during my stay at Matsuura laboratory. His valuable advices on research and chances to join many conferences both domestic and international are my great opportunities. They are experiences which make me understand more about research and information security management. My research could never be done without his kind supports.

Beside my supervisor, I would also like to thank my advisor, Professor Hideyuki Tanaka from Graduate School of Interdisciplinary Information studies, the University of Tokyo, for meaningful and valuable supports, his precious time, advices, discussions, and feedbacks on my research.

I would like to thank all current and past laboratory assistant, Sae Nakano, Naoko Hashizume, and Kayoko Ogura, for their supports since my first contact to Matsuura laboratory while I was in my home country.

Thank you to all present and past members at Matsuura laboratory Takuro Hosoi, Takahiro Matsuda, Peng Yang, Jacob Schuldt, Yasumasa Nakai, Yi Shi, Daiki Chiba, Shaojing Fu, Ken Ichikawa, Young Seok Choi, Takao Murakami, Satsuya Oohata, and Tran Binh Minh for their lovely discussions and comments both related and not related to my research. Moreover they also make my research life at the University of Tokyo be enjoyable with liveliness. I would also like to thank external members during the laboratory's meeting, Chiaki Okada, Takashi Kitagawa, Hitoshi Tanuma, Kouhei Kasamatsu, Takayoshi Hojo, and Ryouta Hishiki for their helpful suggestions on my work.

I am grateful to Panasonic Scholarship and its staffs for the kind financial support during my master course, annual activities, and all supports and advices which let my life in Japan become meaningful.

Finally I would like to thank my beloved family and friends for their support and encouragement. Because of everybody, I could earn many meaningful experiences and smoothly live in Japan from the first day.

Bibliography

- [1] Akihiro Shinozaki, Yusuke Yamamoto, and Shota Yamazaki. ICT 関連経済指標テクニカルペーパー NO.11-1 : 東日本大震災における ICT 関連資本ストックの損害額の推計 (Technical papers on ICT related economic. No. 11-1: Estimation on amount of damage on ICT related capital stock.) Available at http://www.icr.co.jp/ICT/report/TP_201106.pdf, 2011.
- [2] Andrew Odlyzko. Privacy, Economics, and Price Discrimination on the Internet (Extended Abstract). In *ICEC2003: Fifth International Conference on Electronic Commerce*, pages 355–366, 2003.
- [3] Arnoud W.A. Boot and Matej Marinc. The evolving landscape of banking. In *Industrial and Corporate Change*, volume 17, issue 6, pages 1173–1203, 2008.
- [4] Cabineet office, Government of Japan. 産業別資本ストック (Gross Capital Stock by Industry). Available at http://www.esri.cao.go.jp/jp/sna/sonota/minkan/kekka/20110107/h21y_stock_all.xls, 2009.
- [5] Cabinet office, Government of Japan. 月例経済報告等に関する関係閣僚会議震災対応特別会合資料 - 東北地方太平洋沖地震のマクロ経済的影響の分析 (Special cabinet meeting material on monthly economic report due to the earthquake). Available at <http://www5.cao.go.jp/keizai3/getsurei-s/1103.pdf>, 2011.
- [6] Colm Fearon and George Philip. An empirical study of the use of EDI in supermarket chains using a new conceptual framework. In *Journal of Information Technology*, volume 14, issue 1, pages 3–21, 1999.
- [7] Colm Fearon and George Philip. Measuring success of electronic trading in the insurance industry: operationalising the disconfirmation of expectations paradigm. In *Behaviour & Information Technology*, volume 27, issue 6, pages 483–493, 2008.
- [8] Erik Dietzenbacher and Jan A. van der Linder. Sectoral and Spatial linkages in the EC production structure. In *Journal of Regional Science*, volume 37, number 2, pages 235–257, 1997.

- [9] Eva Andrijcic and Barry Horowitz. A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property. In *Risk Analysis*, volume 26, issue 4, pages 907–923, 2006.
- [10] Hal R. Varian. Managing Online Security Risks. In *Economic scene*, *The New York Times*, June 1, 2001. Available at <http://www.nytimes.com/library/financial/columns/060100econ-scene.html>, 2001.
- [11] Hideyuki Tanaka. Geography and Information Security: Does Location Affect Information Security Effort? In *Fourth Forum on Financial Systems and Cyber Security: A Public Policy Perspective*, 2007.
- [12] Hideyuki Tanaka. Quantitative analysis of information security interdependency between industrial sectors. In *ESEM '09: Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement*, pages 574–583, 2009.
- [13] Howard Kunreuther, and Geoffrey Heal. Interdependent Security. In *Journal of Risk and Uncertainty*, volume 26, issue 2–3, pages 231–249, 2003.
- [14] Hulisi Ogut, Nirup Menon, and Srinivasan Raghunathan. Cyber Insurance and IT Security Investment: Impact of Interdependent Risk. In *Workshop on the Economics of Information Security (WEIS05)*, Available at <http://infoecon.net/workshop/schedule.php>, 2005.
- [15] Investopedia Available at <http://www.investopedia.com>
- [16] Jason Dedrick and Kenneth L. Kraemer. The impacts of IT on Firm and Industry Structure: The Personal Computer Industry. In *California Management Review*, volume 47, issue 3, pages 122–142, 2005.
- [17] John Leslie King and Kalle Lyytinen. Automotive Informatics: Information Technology and Enterprise Transformation in the Automobile Industry. In *Transforming enterprise : the economic and social implications of information technology*, Cambridge, Mass. MIT Press, pages 283–312, 2005.
- [18] Joost R. Santos and Yacov Y. Haimes. Modeling the demand reduction input-output (I-O) inoperability due to terrorism of interconnected infrastructures. In *Risk Analysis*, volume 24, issue 6, pages 1437–1451, 2004.

- [19] Joost R. Santos, Yacov Y. Haimes, and Chenyang Lian. A Framework for Linking Cybersecurity Metrics to the Modeling of Macroeconomic Interdependencies. In *Risk Analysis*, volume 27, issue 5, pages 1283–1297, 2007.
- [20] Kjell Hausken. Income, interdependence, and substitution effects affecting incentives for security investment. In *Journal of Accounting and Public Policy*, volume 25, issue 6, pages 629–665, 2006.
- [21] Kunsoo Han, Robert J. Kauffman, and Barrie R. Nault. Information Exploitation and Interorganizational Systems Ownership. In *Journal of Management Information Systems*, volume 21, number 2, pages 109–135, 2004.
- [22] Ministry of Economic, Trade and Industry. 平成 18 年調査関係資料 (2006 Survey of Information Technology). Available at <http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/h18jyojitsu.html>, 2007.
- [23] Ministry of Economic, Trade and Industry 2005. 平成 17 年地域間産業連関表 (Inter-Regional Input-Output Tables 2005). Available at http://www.meti.go.jp/statistics/tyo/tiikiio/result/result_02.html.
- [24] Nicholas G. Carr. IT Doesn’t Matter. In *Harvard Business Review*, pages 41–49, May 2003.
- [25] Office of the manager, National communications system. Supervisory control and data acquisition (SCADA) systems. In *Technical information bulletin 04-1, National communications system*, Available at http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf, 2004.
- [26] Peter Guerra. How Economics and Information Security Affects Cyber Crime and What It Means in the Context of a Global Recession. In *BlackHat USA 2009, Turbo Talk Whitepaper*, Available at <http://www.blackhat.com/presentations/bh-usa-09/GUERRA/BHUSA09-Guerra-EconomicsCyberCrime-PAPER.pdf>, 2009.
- [27] Public Relations and International Affairs Office, Research and Statistics Department Economic and Industrial Policy Bureau, Ministry of Economy, Trade and Industry(METI), Japan. Statistics at METI. Available at http://www.meti.go.jp/english/statistics/pamphlet/h21shokai_en.pdf, March 2010.

- [28] Rainer Böhme and Gaurav Kataria. Models and Measures for Correlation in Cyber-Insurance. In *The Fifth Workshop on the Economics of Information Security*, Cambridge, 26–28 June 2006. Available at <http://weis2006.econinfosec.org/docs/16.pdf>, 2006.
- [29] Remo Häcki and Julian Lighton. The Future of the Networked Company. In *The McKinsey Quarterly*. 3, pages 26–39, 2001.
- [30] Research Institute of Economy, Trade and Industry. 日本産業生産性 (JIP) データベース (Japan Industrial Productivity Database 2008). Available at <http://www.rieti.go.jp/jp/database/JIP2008/index.html>, 2008.
- [31] Richard Pierre; Devinney Timothy. Modular strategies: B2B technology and architectural knowledge. In *University of California, Berkeley, Haas School of Business*, volume 47, number 4, pages 86–113, 2005.
- [32] Ross Anderson. Why Cryptosystems Fail. In *Communications of the ACM*, volume 37, number 11, pages 32–40 Available at <http://www.cl.cam.ac.uk/~rja14/Papers/wcf.pdf>, 1994. ACM.
- [33] Ross Anderson. Why Information Security is Hard - An Economic Perspective. In *Proceedings 17th Annual Computer Security Applications Conference, 2001 (ACSAC 2001)*, pages 358–365 Available at <http://www.acsac.org/2001/papers/110.pdf>, 2001.
- [34] Ross Anderson and Tyler Moore. The Economics of Information Security. In *Science*, volume 314, number 5799, pages 610–613 Available at <http://people.seas.harvard.edu/~tmoore/science-econ.pdf>, 2006.
- [35] Richard Klein and Arun Rai. Interfirm Strategic Information Flows in Logistics Supply Chain Relationships. In *Management Information Systems Quarterly*, volume 33, issue 4, pages 735–762, 2009.
- [36] Sriram Narayanan, Ann S. Maruchek, and Robert B. Handfield. Electronic Data Interchange: Research Review and Future Directions. In *Decision Sciences*, volume 40, issue 1, pages 121–163, 2009.
- [37] The Institute for Information Infrastructure Protection (I3P). Security Solution for the Oil and Gas Industry, Technology Fact Sheet. Inoperability Input-Output Model (IIM). Available at <http://www.dartmouth.edu/~i3p/docs/publications/IIM-factsheet-Feb2007.pdf>, 2007.

- [38] Tridib Bandyopadhyay, Varghese Jacob. and Srinivasan Raghunathan. Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest. In *Information Technology and Management*, volume 11, number 1, pages 7–23. 2010.
- [39] Tony Vila, Rachel Greenstadt, and David Molnar. Why we can’t be bothered to read privacy policies models of privacy economics as a lemons market. In *Proceedings of the 5th international conference on Electronic commerce, ACM International Conference Proceeding Series* volume 50, pages 403–407, 2003. ACM.
- [40] Yacov Y. Haimes, Barry M. Horowitz, James H. Lambert, Joost R. Santos, Chenyang Lian, and Kenneth G. Crowther. Inoperability Input-Output Model for Interdependent Infrastructure Sectors. I: Theory and Methodology. In *Journal of Infrastructure Systems*, volume 11, number 2, pages 67–79, 2005.
- [41] Yacov Y. Haimes, Barry M. Horowitz, James H. Lambert, Joost Santos, Kenneth Crowther, and Chenyang Lian. Inoperability Input-Output Model for Interdependent Infrastructure Sectors. II: Case Studies. In *Journal of Infrastructure Systems*, volume 11, number 2, pages 80–92, 2005.
- [42] Yacov Y Haimes and Clyde G Chittester A Roadmap for Quantifying the Efficacy of Risk Management of Information Security and Interdependent SCADA Systems. In *Journal of Homeland Security and Emergency Management*, volume 2, issue 2, article 12, 2005.
- [43] Yacov Y. Haimes, and Pu Jiang. Leontief-Based Model of Risk in Complex Interconnected Infrastructures. In *International Journal of Networking and Virtual Organizations*, volume 4, issue 3, pages 130–144, 2001.
- [44] Yuko Aoyama and Samuel J. Ratick. Trust, Transactions, and Information Technologies in the U.S. Logistics Industry. In *Economic Geography*, volume 83, issue 2, pages 159–180, 2007.

Publications

Journal

- <1> Bongkot Jenjarrussakul, Kanta Matsuura. A Survey on Information Security Economics. In *Security Management* volume 24, number 3, pages 53–60, January 2011. (Commentaries)

International Conference

- <2> Bongkot Jenjarrussakul, Hideyuki Tanaka, Kanta Matsuura. Empirical Study on Interdependency of Information Security Between Industrial Sectors and Regions. In *Seventh Annual Forum on Financial Information Systems and Cybersecurity: A Public Policy Perspective*, the University of Maryland, January 2011. (Oral Presentation)
- <3> Bongkot Jenjarrussakul, Ryouta Hishiki, Hideyuki Tanaka, Kanta Matsuura, Hideki Imai. Interdependency of Information Security and Its Dependence on IS Multiplier of Sub-industries. In *The 6th International Workshop on Security (IWSEC2011)*, November 2011. (Poster Presentation)
- <4> Bongkot Jenjarrussakul, Hideyuki Tanaka, Kanta Matsuura. Impact on Information Security from the Great East Japan Earthquake on March 11, 2011. In *Eighth Annual Forum on Financial Information Systems and Cybersecurity: A Public Policy Perspective*, the University of Maryland, January 2012. (Oral Presentation)

Domestic conference

- <5> Bongkot Jenjarrussakul, Hideyuki Tanaka, Kanta Matsuura. Empirical Study on Interdependency of Information Security Between Industrial Sectors and Regions. In *2011年暗号と情報セキュリティシンポジウム (SCIS '11)*. IEICE, 小倉, 日本, January 2011.
- <6> Bongkot Jenjarrussakul, Hideyuki Tanaka, Kanta Matsuura. Information Security and Impact from the Great East Japan Earthquake. In *2012年暗号と情報セキュリティシンポジウム (SCIS '12)*. IEICE, 金沢, 日本, January 2012.

Appendix A Results for study on sectoral and regional interdependency of information security

Table A.2–A.13 are used to show results from sectoral perspective. The table’s structure is as follows:

Demand-side region name (ID)	Number of dependent supply-side group (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Hokkaido (A)				1								
Tohoku (B)												
Kanto (C)				1								
Chubu (D)												
Kinki (E)				1								
Chugoku (F)												
Shikoku (G)												
Kyushu (H)												
Okinawa (I)												
Total				3								

Table A.1: Example table shows number of dependent sectors in each region for demand-side sector of X (sector ID)

In table A.1, all listed regions as index along the most left column represents observing demand-side regions for each observing demand-side sector as indicate in the table’s name. The listed *sector ID* as index along the second row of this table represents dependent supply-side sectors regardless region. Value in each intersection between them shows the number of dependent supply-side industrial sectors regardless region which observing demand-side industrial sector in each region shows interdependency when tested.

In example table A.1, we assumes that blank component refer to value of zero for ease

of explanation.

Number of dependent supply-side industrial sectors in each column are summed up and presented in the last row of each table. This last row is indexed as *Total*. It presents values which are the total of number of dependent supply-side groups belong to each industrial sectors as their comlumn index. This means that the values in this row show how much does each supply-side sector is depended by observing demand-side sector X in all regions.

For example, the demand-side sector X in Hokkaido (A) shows interdependency when tested with supply-side sector of metal (04) in one supply-side region (R in particular) . Therefore, the (1,4) component of table A.1 is 1.

Next the demand-side sector X in Kanto (C) shows interdependency when tested with supply-side sector of metal (04) in one supply-side region, and the demand-side sector X in Kinki (E) shows interdependency when tested with supply-side sector of metal(04) in one supply-side region Therefore the (10,4) component of table A.1 is 3.

Demand-side region name (ID)	Number of dependent supply-side group (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Hokkaido (A)	0	0	0	0	0	0	0	0	0	0	0	0
Tohoku (B)	0	0	0	0	0	0	0	0	0	0	0	0
Kanto (C)	0	0	0	0	0	0	0	0	0	0	0	0
Chubu (D)	0	0	0	0	0	0	0	0	0	0	0	0
Kinki (E)	0	0	0	0	0	0	0	0	0	0	0	0
Chugoku (F)	0	0	0	0	0	0	0	0	0	0	0	0
Shikoku (G)	0	0	0	0	0	0	0	0	0	0	0	0
Kyushu (H)	0	0	0	0	0	0	0	0	0	0	0	0
Okinawa (I)	0	0	0	0	0	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0	0	0	0	0	0

*Value of ISBD(%) is about 10-time lower than value of threshold at 0.01%

Table A.2: Number of dependent regions in each sector for demand-side sector of Agriculture (01)*

Demand-side region name (ID)	Number of dependent supply-side group (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Hokkaido (A)	0	0	0	1	0	2	0	1	2	1	0	2
Tohoku (B)	0	0	0	0	0	3	0	1	2	1	0	2
Kanto (C)	0	0	0	1	0	1	0	1	1	1	1	1
Chubu (D)	0	0	0	0	0	3	0	1	2	1	0	2
Kinki (E)	0	0	0	1	0	4	0	1	2	1	0	2
Chugoku (F)	0	0	0	0	0	3	0	1	3	1	0	2
Shikoku (G)	0	0	0	0	0	4	0	1	3	0	0	3
Kyushu (H)	0	0	0	0	0	4	0	1	2	1	0	2
Okinawa (I)	0	0	0	0	0	2	0	1	2	1	0	2
Total	0	0	0	3	0	26	0	9	19	8	1	18

Table A.3: Number of dependent regions in each sector for demand-side sector of Mining (02)

Demand-side region name (ID)	Number of dependent supply-side group (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Hokkaido (A)	1	0	3	2	0	2	0	1	3	1	0	2
Tohoku (B)	1	0	3	1	0	2	0	1	3	1	1	2
Kanto (C)	1	0	4	1	0	3	0	1	2	1	1	1
Chubu (D)	1	0	5	2	0	3	0	1	3	1	1	3
Kinki (E)	0	0	5	1	0	4	0	1	3	1	1	2
Chugoku (F)	2	0	5	1	0	4	0	1	0	5	0	3
Shikoku (G)	1	0	6	2	0	5	0	1	6	0	1	3
Kyushu (H)	1	0	3	1	0	4	0	1	3	0	1	2
Okinawa (I)	3	0	4	1	0	6	0	1	4	1	0	2
Total	11	0	38	12	0	33	0	9	27	11	6	20

Table A.4: Number of dependent regions in each sector for demand-side sector of Food and Beverage (03)

Demand-side region name (ID)	Number of dependent supply-side group (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Hokkaido (A)	0	0	0	7	0	4	0	1	3	2	1	3
Tohoku (B)	0	0	0	6	0	4	0	2	4	2	1	2
Kanto (C)	0	0	0	8	0	4	1	1	3	1	1	1
Chubu (D)	0	0	0	7	0	4	1	1	4	2	2	3
Kinki (E)	0	0	0	7	0	4	1	1	4	1	2	2
Chugoku (F)	0	0	0	6	0	5	1	1	5	2	1	3
Shikoku (G)	0	0	0	6	0	4	0	1	5	1	2	3
Kyushu (H)	0	0	0	6	0	5	1	1	5	1	1	3
Okinawa (I)	0	0	0	8	0	6	1	1	5	1	2	4
Total	0	0	0	61	0	40	6	10	38	13	13	24

Table A.5: Number of dependent regions in each sector for demand-side sector of Metal (04)

Demand-side region name (ID)	Number of dependent supply-side group (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Hokkaido (A)	0	0	0	6	8	7	0	2	5	2	2	5
Tohoku (B)	0	0	0	5	6	6	0	2	4	2	2	4
Kanto (C)	0	0	0	6	7	5	1	1	5	1	1	4
Chubu (D)	0	0	0	5	7	6	0	2	6	3	2	3
Kinki (E)	0	0	0	5	6	5	1	2	5	2	2	4
Chugoku (F)	0	0	0	5	6	5	0	2	5	3	2	5
Shikoku (G)	0	0	0	6	7	6	0	1	6	3	2	6
Kyushu (H)	0	0	0	5	7	5	0	2	5	3	2	5
Okinawa (I)	0	0	0	7	7	6	0	3	6	3	2	5
Total	0	0	0	50	61	51	2	17	47	22	17	41

Table A.6: Number of dependent regions in each sector for demand-side sector of Machinery (05)

Demand-side region name (ID)	Number of dependent supply-side group (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Hokkaido (A)	0	1	0	0	0	6	0	1	2	1	1	2
Tohoku (B)	0	0	0	1	0	6	0	1	3	2	1	2
Kanto (C)	0	0	0	1	0	7	1	1	2	1	1	2
Chubu (D)	0	0	0	3	0	6	0	1	3	2	2	3
Kinki (E)	0	0	0	1	0	7	1	1	3	1	2	2
Chugoku (F)	0	0	0	1	0	6	0	1	4	1	1	3
Shikoku (G)	0	0	0	0	0	6	0	1	5	1	1	3
Kyushu (H)	0	0	0	1	0	6	0	1	4	1	1	3
Okinawa (I)	0	1	0	0	0	6	0	1	2	1	0	2
Total	0	2	0	8	0	56	2	9	28	11	10	22

Table A.7: Number of dependent regions in each sector for demand-side sector of Other manufacturing (06)

Demand-side region name (ID)	Number of dependent supply-side group (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Hokkaido (A)	0	0	0	5	1	5	0	1	2	1	2	2
Tohoku (B)	0	0	0	5	1	4	0	1	3	2	2	2
Kanto (C)	0	0	0	4	1	4	0	1	2	1	1	1
Chubu (D)	0	0	0	5	2	4	0	1	3	1	2	3
Kinki (E)	0	0	0	5	1	4	0	1	3	1	2	2
Chugoku (F)	0	0	0	5	1	5	0	1	5	1	2	3
Shikoku (G)	0	0	0	6	0	6	0	0	5	1	2	3
Kyushu (H)	0	0	0	5	1	5	0	1	3	1	2	2
Okinawa (I)	0	0	0	6	1	6	0	1	4	1	1	2
Total	0	0	0	46	9	43	0	8	30	10	16	20

Table A.8: Number of dependent regions in each sector for demand-side sector of Construction (07)

Demand-side region name (ID)	Number of dependent supply-side group (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Hokkaido (A)	0	0	0	0	0	2	1	1	2	0	1	2
Tohoku (B)	0	0	0	0	0	2	1	1	2	0	1	2
Kanto (C)	0	0	0	0	0	1	1	1	1	1	1	1
Chubu (D)	0	0	0	0	0	2	1	1	2	0	1	2
Kinki (E)	0	0	0	0	0	2	1	1	1	1	2	2
Chugoku (F)	0	0	0	0	0	2	1	1	2	0	1	2
Shikoku (G)	0	0	0	0	0	4	1	1	2	0	1	2
Kyushu (H)	0	0	0	0	0	3	1	1	1	0	1	2
Okinawa (I)	0	0	0	0	0	2	1	1	2	1	0	2
Total	0	0	0	0	0	20	9	9	15	3	9	17

Table A.9: Number of dependent regions in each sector for demand-side sector of Utilities (08)

Demand-side region name (ID)	Number of dependent supply-side group (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Hokkaido (A)	0	0	0	0	0	2	0	1	2	1	2	2
Tohoku (B)	0	0	0	0	0	2	0	1	2	1	2	2
Kanto (C)	0	0	0	0	1	1	1	1	1	1	1	1
Chubu (D)	0	0	0	0	0	2	0	1	2	1	2	2
Kinki (E)	0	0	0	0	0	2	1	1	2	1	2	2
Chugoku (F)	0	0	0	0	0	2	0	1	2	1	2	2
Shikoku (G)	0	0	0	0	0	4	0	1	3	1	2	3
Kyushu (H)	0	0	0	0	0	3	0	1	2	1	2	2
Okinawa (I)	0	0	0	0	2	2	0	1	2	1	2	2
Total	0	0	0	0	3	20	2	9	18	9	17	18

Table A.10: Number of dependent regions in each sector for demand-side sector of Commerce and Logistic (09)

Demand-side region name (ID)	Number of dependent supply-side group (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Hokkaido (A)	0	0	0	0	0	0	0	0	0	0	0	0
Tohoku (B)	0	0	0	0	0	0	0	0	0	0	0	0
Kanto (C)	0	0	0	0	0	0	0	0	0	0	0	1
Chubu (D)	0	0	0	0	0	0	0	0	0	0	0	0
Kinki (E)	0	0	0	0	0	0	0	0	0	0	0	0
Chugoku (F)	0	0	0	0	0	0	0	0	0	0	0	0
Shikoku (G)	0	0	0	0	0	0	0	0	0	0	0	0
Kyushu (H)	0	0	0	0	0	0	0	0	0	0	0	0
Okinawa (I)	0	0	0	0	0	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0	0	0	0	0	1

Table A.11: Number of dependent regions in each sector for demand-side sector of Financial, Insurance, and Real estate (10)

Demand-side region name (ID)	Number of dependent supply-side group (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Hokkaido (A)	0	0	0	0	0	2	0	1	2	1	2	2
Tohoku (B)	0	0	0	0	0	2	0	1	2	2	2	2
Kanto (C)	0	0	0	0	0	3	1	1	1	1	1	1
Chubu (D)	0	0	0	0	0	3	0	1	2	1	2	3
Kinki (E)	0	0	0	0	0	3	1	1	2	1	2	2
Chugoku (F)	0	0	0	0	0	3	0	1	2	1	2	3
Shikoku (G)	0	0	0	0	0	3	0	1	3	1	2	3
Kyushu (H)	0	0	0	0	0	4	0	1	2	1	2	3
Okinawa (I)	0	0	0	0	0	4	0	1	2	1	2	3
Total	0	0	0	0	0	27	2	9	18	10	17	22

Table A.12: Number of dependent regions in each sector for demand-side sector of ICT (11)

Demand-side region name (ID)	Number of dependent supply-side group (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Hokkaido (A)	1	0	2	1	4	5	1	1	3	2	2	2
Tohoku (B)	0	0	2	1	4	4	1	1	4	2	2	2
Kanto (C)	0	0	1	1	3	3	1	1	2	1	1	2
Chubu (D)	0	0	2	2	3	4	1	1	3	2	2	3
Kinki (E)	0	0	1	1	3	4	1	1	3	2	2	2
Chugoku (F)	0	0	1	1	4	6	1	1	5	2	2	3
Shikoku (G)	0	0	1	0	3	6	1	1	6	2	2	3
Kyushu (H)	1	0	1	1	4	6	1	1	5	2	2	3
Okinawa (I)	0	0	2	1	4	6	1	1	5	2	2	3
Total	2	0	13	9	32	44	9	9	36	17	17	23

Table A.13: Number of dependent regions in each sector for demand-side sector of Services (12)

Demand-side region name (ID)	Number of dependent supply-side group (Sector ID)														
	0090	0350	0390	0400	0410	0430	0440	0450	0480	0490	0500	0510	0530		
Hokkaido (A)	2	0	2	2	0	1	2	2	1	2	2	2	1		
Tohoku (B)	2	0	1	2	0	1	2	2	1	2	2	2	1		
Kanto (C)	1	1	1	1	1	1	1	1	0	1	1	1	1		
Chubu (D)	2	0	2	2	0	1	3	2	0	2	2	2	1		
Kinki (E)	2	1	2	1	0	1	2	2	0	2	2	2	1		
Chugoku (F)	2	0	1	2	0	1	3	2	1	3	2	3	1		
Shikoku (G)	2	0	1	2	0	0	3	2	1	2	2	3	1		
Kyushu (H)	2	0	2	2	0	1	2	2	1	2	2	2	1		
Okinawa (I)	1	0	2	2	1	1	2	2	0	2	2	2	1		
Total	16	2	14	16	2	8	20	17	5	18	17	19	9		

Table A.14: Number of dependent regions in each sector for demand-side sector of Financial and Insurance (0400)

Demand-side sector ID	Number of dependent supply-side group (Sector ID)												
	01	02	03	04	05	06	07	08	09	10	11	12	Total
01	0	0	0	0	0	0	0	0	0	0	0	0	0
02	0	0	0	3	0	26	0	9	19	8	1	18	84
03	11	0	38	12	0	33	0	9	27	11	6	20	167
04	0	0	0	61	0	40	6	10	38	13	13	24	205
05	0	0	0	50	61	51	2	17	47	22	17	41	308
06	0	2	0	8	0	56	2	9	28	11	10	22	148
07	0	0	0	46	9	43	0	8	30	10	16	20	182
08	0	0	0	0	0	20	9	9	15	3	9	17	82
09	0	0	0	0	3	20	2	9	18	9	17	18	96
10	0	0	0	0	0	0	0	0	0	0	0	1	1
11	0	0	0	0	0	27	2	9	18	10	17	22	105
12	2	0	13	9	32	44	9	9	36	17	17	23	211
Total	13	2	51	189	105	360	32	98	276	114	123	226	

Table A.15: Total number of dependent supply-side groups belong to each sector by each demand-side sector

Demand-side region name (ID)	Total number of dependent supply-side group (Region ID)											
	A	B	C	D	E	F	G	H	I	Total (All)	Total (Self)	Total (Exclude)
Hokkaido (A)	67	7	52	12	16	9	1	4	0	168	67	101
Tohoku (B)	3	63	59	14	17	6	0	3	0	165	63	102
Kanto (C)	3	8	82	16	21	8	3	4	0	145	82	63
Chubu (D)	2	4	56	70	29	11	2	8	0	182	70	112
Kinki (E)	1	3	48	21	76	14	6	4	0	173	76	97
Chugoku (F)	0	2	49	18	29	67	3	17	0	185	67	118
Shikoku (G)	0	1	47	18	36	22	61	13	0	198	61	137
Kyushu (H)	0	1	48	14	26	19	4	68	0	180	68	112
Okinawa (I)	2	2	47	18	21	12	2	22	67	193	67	126
Total	78	91	488	201	271	168	82	143	67			

Table A.16: Total number of dependent supply-side groups belong each region by each demand-side region

Appendix B Results for changes on interdependency of information security

	Sector ID												
	01	02	03	04	05	06	07	08	09	10	11	12	Total
Case1 with full damage	0	0	1	0	1	5	0	1	3	9	2	0	22
Case1 with reduction in damage	0	0	1	0	1	5	0	1	3	9	2	0	22
Case2 with full damage	0	0	1	2	2	6	1	4	7	10	5	0	38
Case2 with reduction in damage	0	0	1	2	2	6	1	4	7	10	5	0	38

Table B.1: Number of different supply-side groups from sectoral perspective when tested interdependency with sectors in *Tohoku(B)* with damage in Tohoku.

	Region ID									
	A	B	C	D	E	F	G	H	I	Total
Case1 with full damage	3	8	5	3	2	0	0	1	0	22
Case1 with reduction in damage	3	8	5	3	2	0	0	1	0	22
Case2 with full damage	3	14	11	3	6	0	0	1	0	38
Case2 with reduction in damage	3	14	11	3	6	0	0	1	0	38

Table B.2: Number of different supply-side groups from regional perspective when tested interdependency with sectors in *Tohoku(B)* with damage in Tohoku.

	Sector ID												
	01	02	03	04	05	06	07	08	09	10	11	12	Total
Case1 with full damage	0	0	0	0	0	0	0	0	0	0	0	1	1
Case1 with reduction in damage	0	0	0	0	0	0	0	0	0	0	0	1	1
Case2 with full damage	0	0	0	0	0	0	0	0	0	0	0	1	1
Case2 with reduction in damage	0	0	0	0	0	0	0	0	0	0	0	1	1

Table B.3: Number of different supply-side groups from sectoral perspective when tested interdependency with sectors in $Kanto(C)$ with damage in Tohoku.

	Region ID									
	A	B	C	D	E	F	G	H	I	Total
Case1 with full damage	0	1	0	0	0	0	0	0	0	1
Case1 with reduction in damage	0	1	0	0	0	0	0	0	0	1
Case2 with full damage	0	1	0	0	0	0	0	0	0	1
Case2 with reduction in damage	0	1	0	0	0	0	0	0	0	1

Table B.4: Number of different supply-side groups from regional perspective when tested interdependency with sectors in $Kanto(C)$ with damage in Tohoku.

	Sector ID												
	01	02	03	04	05	06	07	08	09	10	11	12	Total
Case1 with full damage	0	0	0	0	0	0	0	0	0	0	0	0	0
Case1 with reduction in damage	0	0	0	0	0	0	0	0	0	0	0	0	0
Case2 with full damage	0	0	0	0	0	0	0	0	1	0	0	0	1
Case2 with reduction in damage	0	0	0	0	0	0	0	0	1	0	0	0	1

Table B.5: Number of different supply-side groups from sectoral perspective when tested interdependency with sectors in $Kyushu(H)$ with damage in Tohoku.

	Region ID									
	A	B	C	D	E	F	G	H	I	Total
Case1 with full damage	0	0	0	0	0	0	0	0	0	0
Case1 with reduction in damage	0	0	0	0	0	0	0	0	0	0
Case2 with full damage	0	0	0	1	0	0	0	0	0	1
Case2 with reduction in damage	0	0	0	1	0	0	0	0	0	1

Table B.6: Number of different supply-side groups from regional perspective when tested interdependency with sectors in $Kyushu(H)$ with damage in Tohoku.

	Sector ID												
	01	02	03	04	05	06	07	08	09	10	11	12	Total
Case1 with full damage	0	0	0	0	0	0	0	0	1	0	0	0	1
Case1 with reduction in damage	0	0	0	0	0	0	0	0	1	0	0	0	1
Case2 with full damage	0	0	0	0	0	0	0	1	1	1	0	0	3
Case2 with reduction in damage	0	0	0	0	0	0	0	1	1	1	0	0	3

Table B.7: Number of different supply-side groups from sectoral perspective when tested interdependency with sectors in $Tohoku(B)$ with damage in Kanto.

	Region ID									
	A	B	C	D	E	F	G	H	I	Total
Case1 with full damage	0	0	0	1	0	0	0	0	0	1
Case1 with reduction in damage	0	0	0	1	0	0	0	0	0	1
Case2 with full damage	0	0	2	1	0	0	0	0	0	3
Case2 with reduction in damage	0	0	2	1	0	0	0	0	0	3

Table B.8: Number of different supply-side groups from regional perspective when tested interdependency with sectors in $Tohoku(B)$ with damage in Kanto.

	Sector ID												
	01	02	03	04	05	06	07	08	09	10	11	12	Total
Case1 with full damage	0	0	1	1	0	0	1	0	0	0	0	2	5
Case1 with reduction in damage	0	0	1	1	0	0	1	0	0	0	0	2	5
Case2 with full damage	0	0	1	1	1	1	2	0	0	0	0	2	8
Case2 with reduction in damage	0	0	1	1	1	1	2	0	0	0	0	2	8

Table B.9: Number of different supply-side groups from sectoral perspective when tested interdependency with sectors in $Kanto(C)$ with damage in Kanto.

	Region ID									
	A	B	C	D	E	F	G	H	I	Total
Case1 with full damage	1	1	1	1	1	0	0	0	0	5
Case1 with reduction in damage	1	1	1	1	1	0	0	0	0	5
Case2 with full damage	1	1	3	1	1	1	0	0	0	8
Case2 with reduction in damage	1	1	3	1	1	1	0	0	0	8

Table B.10: Number of different supply-side groups from regional perspective when tested interdependency with sectors in $Kanto(C)$ with damage in Kanto.

	Sector ID												
	01	02	03	04	05	06	07	08	09	10	11	12	Total
Case1 with full damage	0	0	0	0	0	0	0	0	0	0	0	0	0
Case1 with reduction in damage	0	0	0	0	0	0	0	0	0	0	0	0	0
Case2 with full damage	0	0	0	0	0	0	0	0	1	0	0	0	1
Case2 with reduction in damage	0	0	0	0	0	0	0	0	1	0	0	0	1

Table B.11: Number of different supply-side groups from sectoral perspective when tested interdependency with sectors in $Kyushu(H)$ with damage in Kanto.

	Region ID									
	A	B	C	D	E	F	G	H	I	Total
Case1 with full damage	0	0	0	0	0	0	0	0	0	0
Case1 with reduction in damage	0	0	0	0	0	0	0	0	0	0
Case2 with full damage	0	0	0	1	0	0	0	0	0	1
Case2 with reduction in damage	0	0	0	1	0	0	0	0	0	1

Table B.12: Number of different supply-side groups from regional perspective when tested interdependency with sectors in $Kyushu(H)$ with damage in Kanto.